

GUTRIDE SAFIER LLP

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

Kali R. Backer (State Bar No. 342492)

kali@gutridesafier.com

100 Pine Street, Suite 1250

San Francisco, CA 94111

Telephone: (415) 639-9090

Facsimile: (415) 449-6469

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

VISHAL SHAH and CHRISTINE WILEY, on
behalf of themselves, the general public, and
those similarly situated,

Plaintiffs,

v.

MYFITNESSPAL, INC.,

Defendant.

CASE NO.

CLASS ACTION COMPLAINT FOR
INVASION OF PRIVACY; INTRUSION
UPON SECLUSION; WIRETAPPING IN
VIOLATION OF THE CALIFORNIA
INVASION OF PRIVACY ACT
(CALIFORNIA PENAL CODE § 631); USE
OF A PEN REGISTER IN VIOLATION OF
THE CALIFORNIA INVASION OF
PRIVACY ACT (CALIFORNIA PENAL
CODE § 638.51); COMMON LAW FRAUD,
DECEIT AND/OR
MISREPRESENTATION; UNJUST
ENRICHMENT; AND TRESPASS TO
CHATTELS

JURY TRIAL DEMANDED

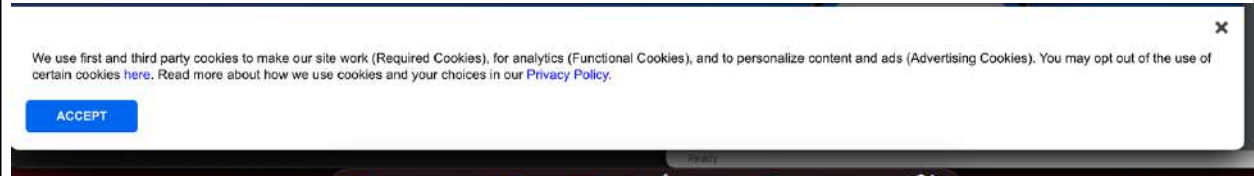
TABLE OF CONTENTS

INTRODUCTION	1
THE PARTIES.....	3
JURISDICTION AND VENUE	3
WEBSITE TERMS AND CONDITIONS OF USE	4
SUBSTANTIVE ALLEGATIONS	4
A. Defendant Programmed the Website to Include Third-Party Resources that Utilize Cookie Trackers.	4
B. Defendant Falsely Informed Users That They Could "Opt Out" of Certain Cookies in Use on the Website.	19
C. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Website.	29
1. Facebook Cookies	29
2. Google Cookies.....	33
3. TikTok Cookies	38
4. Additional Third-Party Cookies.....	41
D. The Private Communications Collected are Valuable.	42
PLAINTIFFS' EXPERIENCES	44
CLASS ALLEGATIONS	51
CAUSES OF ACTION	53
First Cause of Action: Invasion of Privacy	53
Second Cause of Action: Intrusion Upon Seclusion.....	56
Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631).....	57
Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)	62
Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation.....	64
Sixth Cause of Action: Unjust Enrichment.....	66
Seventh Cause of Action: Trespass to Chattels	67

1 Plaintiffs Vishal Shah and Christine Wiley (“Plaintiffs”) bring this action on behalf of
 2 themselves, the general public, and all others similarly situated against MyFitnessPal, Inc.
 3 (“Defendant” or “MyFitnessPal”). Plaintiffs’ allegations against Defendant are based upon
 4 information and belief, and upon investigation of Plaintiffs’ counsel, except for allegations
 5 specifically pertaining to Plaintiffs, which are based upon Plaintiffs’ personal knowledge.

6 **INTRODUCTION**

7 1. This Class Action Complaint concerns an egregious privacy violation and total
 8 breach of consumer trust in violation of California law. When consumers visit Defendant’s
 9 website (www.myfitnesspal.com, the “Website”), Defendant displays to them a popup cookie
 10 consent banner. Defendant’s cookie banner discloses that the Website uses cookies but expressly
 11 gives users the option to control how they are tracked and how their personal data is used.
 12 Defendant assures visitors that they can choose to “opt out of the use of certain cookies here[.]”
 13 where the word “here” is a hyperlink that users can click or select, as shown in the following
 14 screenshot:



16
 17
 18 2. Like most internet websites, Defendant designed the Website to include resources
 19 and programming scripts from third parties that cause those parties to place cookies and other
 20 similar tracking technologies on visitors’ browsers and devices and/or transmit cookies along
 21 with user data. However, unlike other websites, Defendant’s Website offers consumers a choice
 22 to browse without being tracked, followed, and targeted by third party data brokers and
 23 advertisers. But, Defendant’s promises are outright lies, designed to lull users into a false sense
 24 of security. Even after users elect to opt out of cookies by following the “here” link, then
 25 adjusting all available settings to opt out of, decline, or reject all categories of cookies, including
 26 Functional and Advertising cookies (other than those required for the operation of the Website),
 27 Defendant surreptitiously causes several third parties—including Meta Platforms, Inc.
 28 (Facebook), Google LLC (DoubleClick and Google Analytics), ByteDance Ltd. (TikTok),

1 Amazon.com, Inc. (c.amazon-adsystem), and The Trade Desk, Inc. (adsrvr.org) (the “Third
2 Parties”)—to place and/or transmit cookies that track users’ website browsing activities and
3 eavesdrop on users’ private communications on the Website.

4 3. Contrary to their express declination or rejection of cookies and tracking
5 technologies on the Website, Defendant nonetheless caused cookies, including the Third Parties’
6 cookies, to be sent to Plaintiffs and other visitors’ browsers, stored on their devices, and
7 transmitted to the Third Parties along with user data. These third-party cookies permitted the
8 Third Parties to track and collect data in real time regarding Website visitors’ behaviors and
9 communications, including their browsing history, visit history, website interactions, user input
10 data, demographic information, interests and preferences, shopping behaviors, device
11 information, referring URLs, session information, user identifiers, and/or geolocation data.

12 4. The Third Parties analyze and aggregate this user data across websites and time
13 for their own purposes and financial gain, including, creating consumer profiles containing
14 detailed information about a consumer’s behavior, preferences, and demographics; creating
15 audience segments based on shared traits (such as Millennials, tech enthusiasts, etc.); and
16 performing targeted advertising and marketing analytics. Further, the Third Parties share user
17 data and/or user profiles to unknown parties to further their financial gain.

18 5. This type of tracking and data sharing is exactly what the Website visitors who
19 clicked or selected the “here” link on the Website’s cookie consent banner, then adjusted all
20 available settings to decline or reject all such cookies, sought to avoid. Defendant falsely told
21 Website users that they could “opt out” of the use and placement of such cookies, or otherwise
22 “choose” whether such cookies are used on the Website, thereby avoiding tracking and data
23 sharing when they browsed the Website. Despite receiving notice of consumers’ express
24 declination of consent, Defendant defied it and violated state statutes, and tort duties.

THE PARTIES

6. Plaintiff Vishal Shah is, and was at all relevant times, an individual and resident of San Jose, California. Plaintiff Shah intends to remain in California and makes his permanent home there.

7. Plaintiff Christine Wiley is, and was at all relevant times, an individual and resident of California. Plaintiff Wiley intends to remain in California and makes her permanent home there.

8. Defendant MyFitnessPal, Inc. is a Delaware corporation with its headquarters and principal place of business in Austin, Texas.

JURISDICTION AND VENUE

9. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2). The aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs; and Plaintiffs and Defendant are citizens of different states.

10. The injuries, damages and/or harm upon which this action is based, occurred or arose out of activities engaged in by Defendant within, affecting, and emanating from, the State of California. Defendant regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and services provided to persons in the State of California. Defendant has engaged, and continues to engage, in substantial and continuous business practices in the State of California.

11. Further, the Private Communications and data which Defendant causes to be transmitted to Third Parties are routed through servers located in California.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in the state of California, including within this District.

13. Plaintiffs accordingly allege that jurisdiction and venue are proper in this Court.

WEBSITE TERMS AND CONDITIONS OF USE

14. The Website contains a Terms and Conditions of Use (“Terms”) with an arbitration provision purporting to require “any and all disputes” between website visitors and Defendant to be resolved by binding arbitration. However, no agreement to arbitrate was ever formed between either of the Plaintiffs and Defendant.

15. The Website’s Terms are available on the Website but accessible only via an inconspicuous link displayed in small font at the bottom of the Website after all the main content. Moreover, Defendant does not require Website users to read or agree to the Terms before browsing the Website. In fact, Website users cannot even interact with the Website (to see the link to the Terms or to review the Terms) until a user makes their cookie preference selection in the cookie consent banner.

16. When Plaintiffs visited the Website, they did not see or otherwise assent to the Terms before choosing to reject all cookies in the Your Choices window, except the “Required Cookies,” which Plaintiffs were unable to reject, before proceeding to browse the Website. Plaintiffs did not sign up for an account on the Website or the digital app. Accordingly, Plaintiffs made no agreement to arbitrate their privacy claims.

SUBSTANTIVE ALLEGATIONS

A. Defendant Programmed the Website to Include Third-Party Resources that Utilize Cookie Trackers.

17. Every website, including the Website, is hosted by a server that sends and receives communications in the form of HTTP requests, such as “GET” or “POST” requests, to and from Internet users’ browsers. For example, when a user clicks on a hyperlink on the Website, the user’s browser sends a “GET” request to the Website’s server. The GET request tells the Website server what information is being requested (e.g., the URL of the webpage being requested) and instructs the Website’s server to send the information back to the user (e.g., the content of the webpage being requested). When the Website server receives an HTTP request, it processes that request and sends back an HTTP response. The HTTP request includes the client’s IP address so that the Website server to knows where to send the HTTP response.

1 18. An IP address (Internet Protocol address) is a unique numerical label assigned to
2 each device connected to a network that uses the Internet Protocol for communication, typically
3 expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4
4 addresses). IP addresses can identify the network a device is on and the specific device within
5 that network. Public IP addresses used for internet-facing devices reveal geographical locations,
6 such as country, city, or region, through IP geolocation databases.

7 19. As a result, Defendant knew that the device or devices used by Plaintiffs and
8 Class members to access the Website were located in California.

9 20. Defendant voluntarily integrated “third-party resources” from the Third Parties
10 into its Website programming. “Third-party resources” refer to tools, content or services
11 provided by third-parties, such as analytics tools, advertising networks, or payment processors,
12 that a website developer utilizes by embedding scripts, styles, media, or application
13 programming interface (API) into the website’s code. Defendant’s use of the third-party
14 resources on the Website is done so pursuant to agreements between Defendant and those Third
15 Parties.

16 21. The Website causes users’ devices to store and/or transmit both first-party and
17 third-party tracking cookies. Cookies are small text files sent by a website server to a user’s web
18 browser and stored locally on the user’s device. As described below, cookies generally contain
19 a unique identifier which causes the website to recognize and differentiate individual users.
20 Cookie files are sent back to the website server along with HTTP requests, causing the website
21 to identify the device making the requests, and to record a session showing how the user interacts
22 with the website.

23 22. First-party cookies are those that are placed on the user’s device directly by the
24 web server with which the user is knowingly communicating (in this case, the Website’s server).
25 First-party cookies are used to track users when they repeatedly visit the same website.

26 23. A third-party cookie is set by a third-party domain/webserver (e.g.,
27 www.google.com; www.facebook.com; analytics.tiktok.com; etc.). When the user’s browser
28

1 loads a webpage (such as a webpage of the Website) containing embedded third-party resources,
2 the third-parties' programming scripts typically issue HTTP commands to determine whether
3 the third-party cookies are already stored on the user's device and to cause the user's browser to
4 store those cookies on the device if they do not yet exist. Third-party cookies include an identifier
5 that allows the third-party to recognize and differentiate individual users across websites
6 (including the Website) and across multiple browsing sessions.

7 24. As described further below, the third-party cookies stored on and/or loaded from
8 users' devices when they interact with the Website are transmitted to those third parties, causing
9 them to surreptitiously track in real time and collect Website users' personal information, such
10 as their browsing activities and private communications with Defendant, including the following:

- 11 • **Browsing History:** Information about the webpages a Website user visits,
12 including the URLs, titles, and keywords associated with the webpages viewed,
13 time spent on each page, and navigation patterns;
- 14 • **Visit History:** Information about the frequency and total number of visits
15 to the Website;
- 16 • **Website Interactions:** Data on which links, buttons, or ads on the
17 Website that a user clicks;
- 18 • **User Input Data:** The information the user entered into the Website's
19 form fields, including search queries, the user's name, age, gender, email address,
20 location, and/or payment information;
- 21 • **Demographic Information:** Inferences about age, gender, and location
22 based on browsing habits and interactions with Website content;
- 23 • **Interests and Preferences:** Insights into user interests based on the types
24 of Website content viewed, products searched for, or topics engaged with;
- 25 • **Shopping Behavior:** Information about the Website products viewed or
26 added to shopping carts;

- **Device Information:** Details about the Website user's device, such as the type of device (mobile, tablet, desktop), operating system, and browser type;
- **Referring URL:** Information about the website that referred the user to the Website;
- **Session Information:** Details about the user's current Website browsing session, including the exact date and time of the user's session, the session duration and actions taken on the Website during that session;
- **User Identifiers:** A unique ID that is used to recognize and track a specific Website user across different websites over time; and/or
- **Geolocation Data:** General location information based on the Website user's IP address or GPS data, if accessible, including whether the user is located in California.

(Collectively, the browsing activities and private communications listed in the bullet points above shall be referred to herein as "Private Communications").

25. Third-party cookies can be used for a variety of purposes, including (i) analytics (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing campaigns); (ii) personalization (e.g., remembering a user's browsing history and purchase preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering targeted advertisements based on the user's consumer profile (i.e., an aggregated profile of the user's behavior, preferences, and demographics); and (iv) social media integration (e.g., enabling sharing of users' activities with social media platforms). Ultimately, third-party cookies are utilized to boost website performance and revenue through the collection, utilization, and dissemination of user data.

26. Defendant's primary product is a smartphone application and website of the same name designed to help users track their calorie intake, exercise, and overall health and fitness goals. Defendant owns and operates the Website, which promotes the smartphone application and allows users to access certain application functions through the Website itself. As they

1 interact with the Website (e.g., by entering data into forms, clicking on links, and making
2 selections), Website users communicate Private Communications to Defendant, including their
3 browsing history, visit history, website interactions, user input data, demographic information,
4 interests and preferences, shopping behaviors, device information, referring URLs, session
5 information, user identifiers, and/or geolocation data.

6 27. Defendant chose to install or integrate its Website with resources from the Third
7 Parties that, among other things, use cookies. Thus, when consumers visit the Website, both first-
8 party cookies and third-party cookies are placed on their devices and/or transmitted. This is
9 caused by software code that Defendant incorporates into its Website, or that Defendant causes
10 to be loaded. Because Defendant controls the software code of its Website, and is capable of
11 determining whether a user is accessing the Website from California, it has complete control
12 over whether first-party and third-party cookies are placed on its California users' devices and/or
13 transmitted to third parties.

14 28. Defendant explained the third-party cookies it used on the Website as follows in
15 its Privacy Policy:

16 Cookies serve a wide variety of purposes. Cookies are pieces of data stored in your
17 web browser that are transmitted to websites to remember your browser over time
18 and distinguish it from other users. Cookies are used to personalize your web
19 experience and for security, analytics, marketing, and interest-based advertising.
20 Our cookies are placed and read by our web servers, while other cookies are placed
21 and read by other companies' web servers. Information on specific cookies is found
22 on our website via the adchoices link. You can block and control cookies using the
23 information noted in this section. If you block all cookies, certain functionality on
24 our Website will not work.

25 ...

26 Pixels are extremely small image files that, when loaded by your web browser,
27 cause the browser to make a network request to the party corresponding to the pixel.
28 If that party's cookies are currently stored in your browser, those cookies will be
transmitted with the request. Beacons can be used on web pages for advertising or
to confirm the opening of a marketing email. When used in conjunction with
cookies for interest-based-advertising, the cookie controls above can be used to
control the purpose for which they are used.

...

We use cookies, pixels (including email pixels), mobile device and advertising IDs, general location data, Fitness and Wellness Data, app or service usage data and data from third- party wearables, connected devices or sensors that integrate with our Services for purposes of interest-based and cross-app, cross-device advertising.¹

29. Defendant also defines the categories of cookies in use on its Website in its Privacy Policy as follows:

Required Cookies. These strictly necessary cookies are used for core functionality, and recognize when you are signed in, are necessary for security, and enforce your privacy preferences. Without these cookies, some functionality on our Website may fail...

Functional Cookies. These cookies help to improve the Website by allowing us to understand how the Website is used and how the Website performs. These cookies include analytics and measurement...

Advertising Cookies. These cookies help us and other parties personalize ads that are shown to you on the Services, as well as on other websites. If enabled, these cookies will allow third parties engaged in interest-based advertising on our Website to recognize your browser software on other websites too.

30. Defendant further defines the categories of cookies in use on its Website in its Your Choices Regarding Cookies on this Site window (the “Your Choices” window) which is presented to users when they click or select the “here” link in the popup cookie consent banner, as follows:

Required Cookies

These cookies are required to enable core site functionality.

Functional Cookies

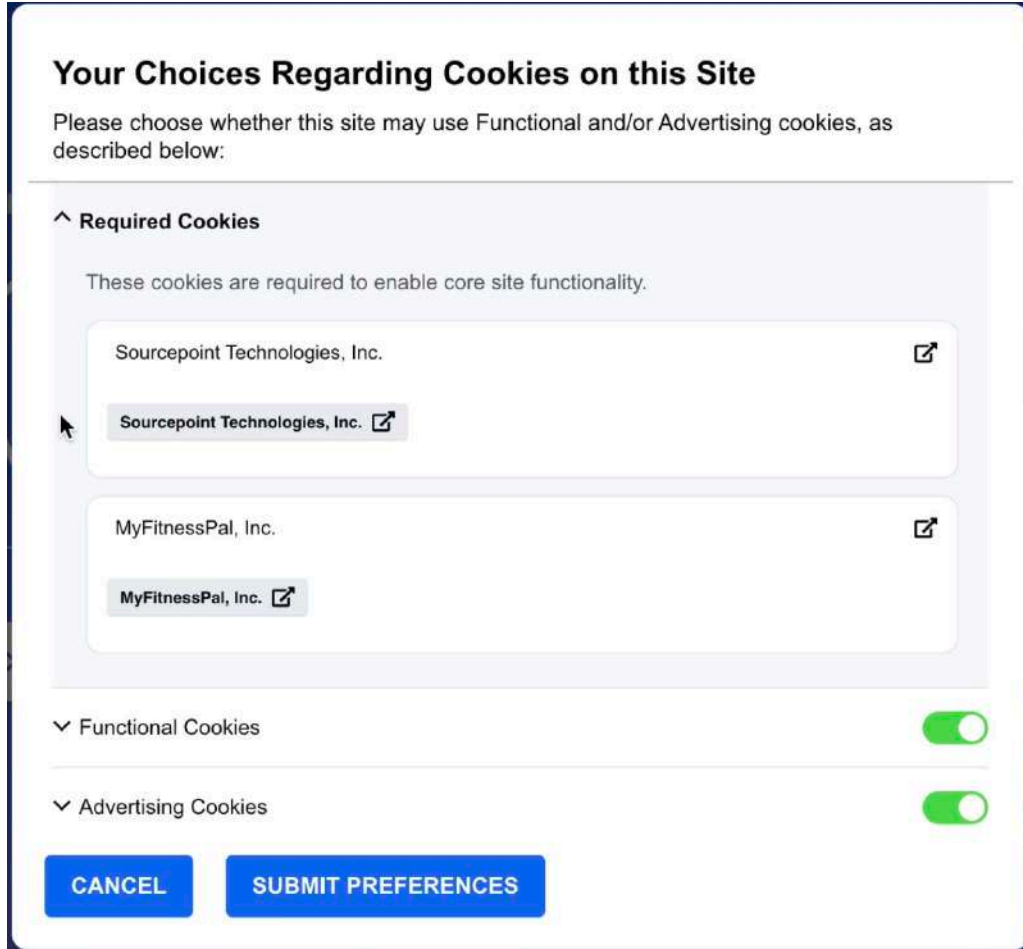
These cookies allow us to analyze site usage so we can measure and improve performance.

Advertising Cookies

These cookies are used by advertising companies to serve ads that are relevant to your interests.

¹ MyFitnessPal Website Privacy Policy (Effective: December 18, 2020) (current version available at <https://www.myfitnesspal.com/privacy-policy>) (the “Privacy Policy”). Defendant has subsequently updated its Privacy Policy but, based on information and belief, this version was in effect at the time of Plaintiffs’ choice to “opt out” of cookies on the Website.

31. Defendant also identified the specific third-party cookies in use on the Website for each category of cookies in its Your Choices window. In particular, Defendant identified only two providers of “Required Cookies” as shown in the following screenshot:



32. Further, Defendant identified Facebook, Google, and Amazon as providers of “Functional Cookies” in use on the Website as shown in the following screenshots:

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28


Your Choices Regarding Cookies on this Site


Please choose whether this site may use Functional and/or Advertising cookies, as described below:


▼ Required Cookies


^ Functional Cookies ☒


These cookies allow us to analyze site usage so we can measure and improve performance.

Adobe Advertising Cloud 

Adobe Advertising Cloud 

Amazon Cloudfront 

Amazon Cloudfront 

Amazon Web Services 

CANCEL

SUBMIT PREFERENCES

- 11 -

CLASS ACTION COMPLAINT

Your Choices Regarding Cookies on this Site

Please choose whether this site may use Functional and/or Advertising cookies, as described below:

Adobe Advertising Cloud



Adobe Advertising Cloud 

Amazon Cloudfront



Amazon Cloudfront 

Amazon Web Services



Amazon Web Services 

AMP










AMP 

CANCEL

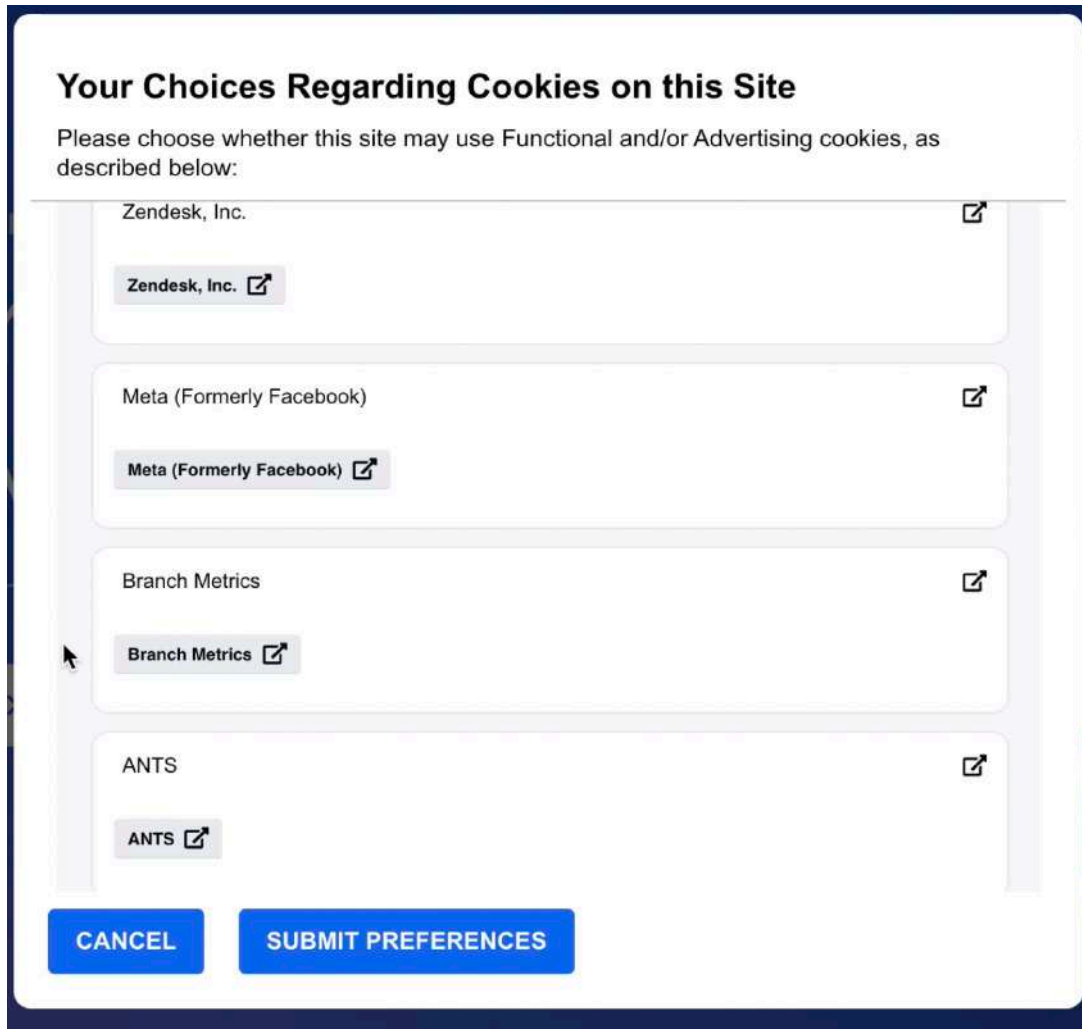
SUBMIT PREFERENCES

Your Choices Regarding Cookies on this Site

Please choose whether this site may use Functional and/or Advertising cookies, as described below:

DistroScale	
DistroScale 	
Google, Inc.	
Google, Inc. 	
jsdelivr	
jsdelivr 	
LiveRamp, Inc.	

CANCEL **SUBMIT PREFERENCES**



33. Additionally, Defendant identified Facebook, Google, Amazon, and TradeDesk as providers of “Advertising Cookies” in use on the Website as shown in the following screenshots:

Your Choices Regarding Cookies on this Site


Please choose whether this site may use Functional and/or Advertising cookies, as described below:


▼ Required Cookies


▼ Functional Cookies ☒


^ Advertising Cookies ☒

These cookies are used by advertising companies to serve ads that are relevant to your interests.

A.Mob 

A.Mob 

AcuityAds Inc. 

AcuityAds Inc. 

CANCEL **SUBMIT PREFERENCES**

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25


26


27


28


Your Choices Regarding Cookies on this Site


Please choose whether this site may use Functional and/or Advertising cookies, as described below:


ADYOU LIKE SA 


Amazon Advertising 

Amazon Advertising 

Amobee Inc. 

Amobee Inc. 

Appier PTE Ltd 

Appier PTE Ltd 

CANCEL

SUBMIT PREFERENCES

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25


26


27


28


Your Choices Regarding Cookies on this Site


Please choose whether this site may use Functional and/or Advertising cookies, as described below:


Getintent USA, inc. 


Getintent USA, inc. 


Google, Inc. 

Google, Inc. 

GumGum, Inc. 

GumGum, Inc. 

Hybrid Adtech GmbH 

Hybrid Adtech GmbH 

CANCEL

SUBMIT PREFERENCES

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25


26


27


28


Your Choices Regarding Cookies on this Site


Please choose whether this site may use Functional and/or Advertising cookies, as described below:


Teads 


Teads 


The Trade Desk 

The Trade Desk 

travel audience GmbH 

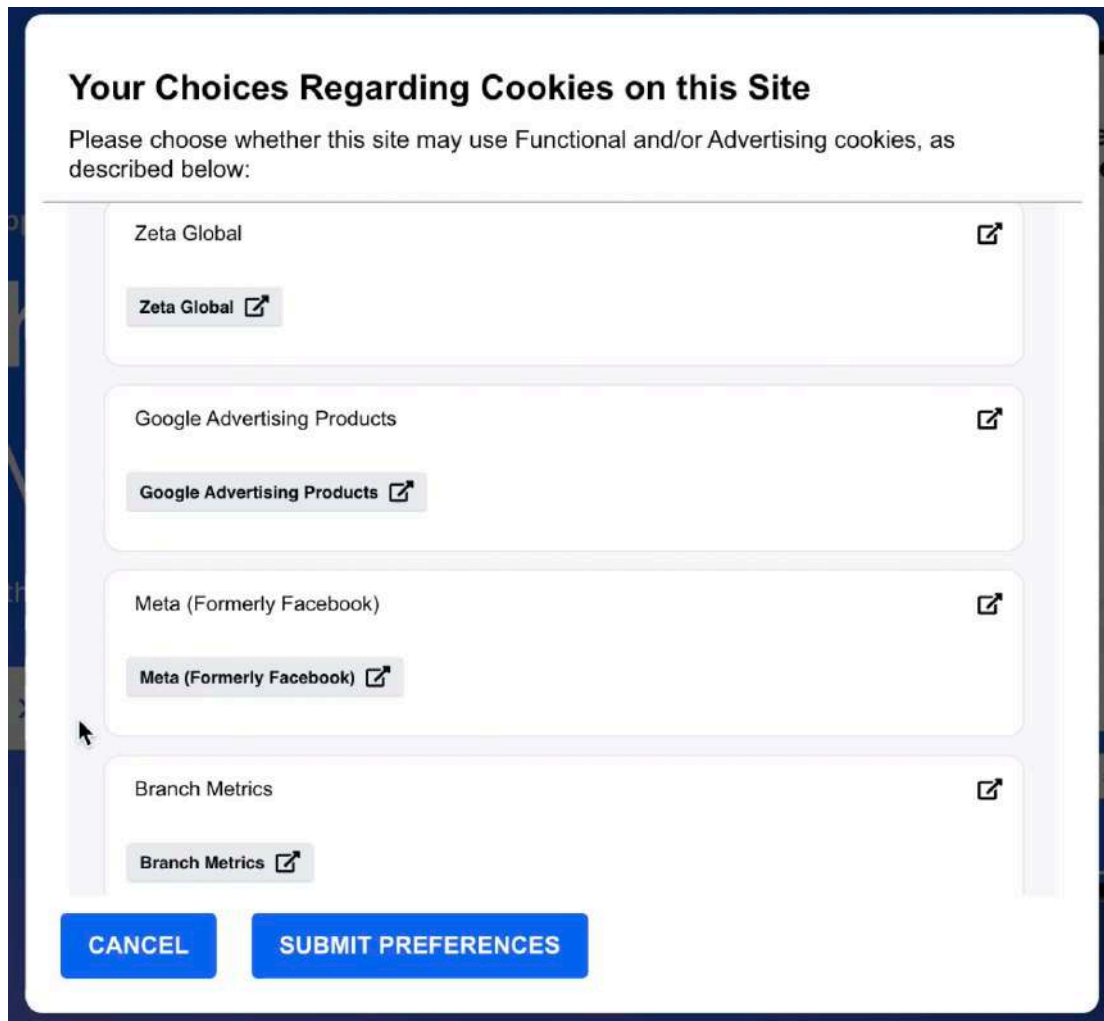
travel audience GmbH 

TripleLift, Inc. 

TripleLift, Inc. 

CANCEL

SUBMIT PREFERENCES

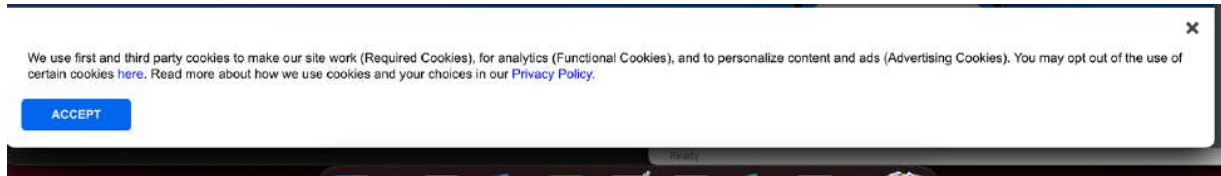


34. Defendant failed to disclose its use of TikTok cookies in any of the categories on the Your Choices window but as alleged below, TikTok’s cookies are used for advertising purposes.

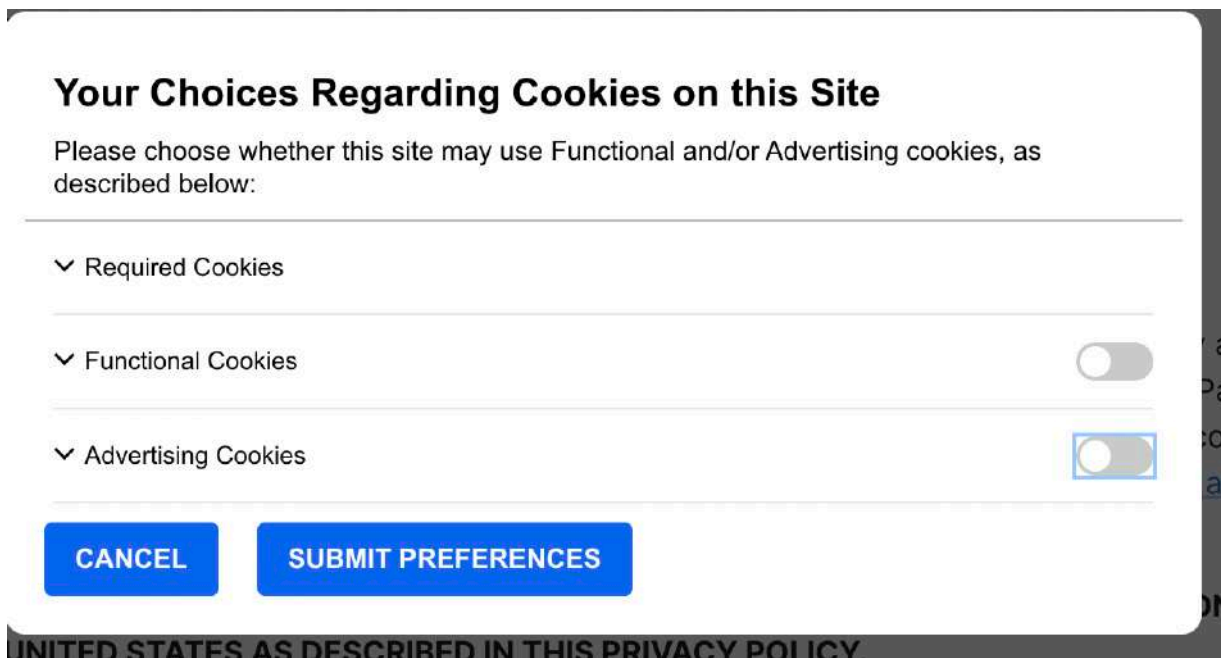
B. Defendant Falsely Informed Users That They Could “Opt Out” of Certain Cookies in Use on the Website.

35. When Plaintiffs and other consumers in California visited the Website, the Website immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the cookie consent banner stated, “We use first and third party cookies to make our site work (Required Cookies), for analytics (Functional Cookies), and to personalize content and ads (Advertising Cookies). You may opt out of the use of certain cookies here[,]” where the

word “[here](#)” was a hyperlink that users could select or click, as shown in the following screenshot from the Website:



36. Plaintiffs and other Website users who indicated their choice and/or agreement to “opt out of the use of certain cookies” by clicking or selecting the “[here](#)” link were then directed to the Your Choices window, which further stated that users could “choose whether this site may use Functional and/or Advertising cookies[.]” The Your Choices window featured toggle switches that users could adjust to opt out of, decline, or otherwise reject such cookies, along with explanations of those cookies and examples of those cookies, as shown in these screenshots:



Your Choices Regarding Cookies on this Site

Please choose whether this site may use Functional and/or Advertising cookies, as described below:

^ Required Cookies

These cookies are required to enable core site functionality.

Sourcepoint Technologies, Inc.



Sourcepoint Technologies, Inc. 

MyFitnessPal, Inc.



MyFitnessPal, Inc. 

✓ Functional Cookies



✓ Advertising Cookies



CANCEL

SUBMIT PREFERENCES

Your Choices Regarding Cookies on this Site

Please choose whether this site may use Functional and/or Advertising cookies, as described below:

^ Functional Cookies



These cookies allow us to analyze site usage so we can measure and improve performance.

Adobe Advertising Cloud



Adobe Advertising Cloud 

Amazon Cloudfront



Amazon Cloudfront 

Amazon Web Services



Amazon Web Services 

CANCEL

SUBMIT PREFERENCES

Your Choices Regarding Cookies on this Site

Please choose whether this site may use Functional and/or Advertising cookies, as described below:

^ Advertising Cookies

These cookies are used by advertising companies to serve ads that are relevant to your interests.

A.Mob 

A.Mob 

AcuityAds Inc. 

AcuityAds Inc. 

Adelphic 

Adelphic 

CANCEL

SUBMIT PREFERENCES

37. Plaintiffs and other Website users who adjusted all available settings on the Your Choices window, indicating their choice and/or agreement to “opt out” of, decline, or reject all Functional and Advertising cookies and tracking technologies in use on the Website, could then continue to browse the Website, as the popup cookie consent banner and Your Choices window disappeared.

38. Defendant’s popup cookie consent banner and Your Choices window led Plaintiffs, and all those Website users similarly situated, to believe that they had opted out of, declined, or rejected all categories of cookies, including Functional and Advertising cookies, other than those required for the operation of the Website, especially those used “for analytics...and to personalize content and ads[.]” The banner and window further reasonably


1 led Plaintiffs and those Website users similarly situated to believe that Defendant would not
2 allow third parties, through cookies, to access their Private Communications with the Website,
3 including their browsing history, visit history, website interactions, user input data,
4 demographic information, interests and preferences, shopping behaviors, device information,
5 referring URLs, session information, user identifiers, and/or geolocation data, upon adjusting
6 settings to “opt out” of, decline, or otherwise reject all categories of non-required cookies,
7 including Functional and Advertising cookies, as described above.

8 39. Defendant’s representations, however, were false. In truth, Defendant did not
9 abide by Plaintiffs’ or other users’ wishes. When Plaintiffs and other users selected or clicked
10 the “here” link, then adjusted all available settings to “opt out” of, decline, or reject non-
11 required cookies on the Your Choices window, they provided notice to Defendant that they did
12 not consent to the placement or transmission of third-party cookies that would allow those
13 parties to obtain their Private Communications with the Website. Nevertheless, Defendant
14 caused the Third-Party tracking cookies, including Functional and Advertising cookies, to be
15 placed on Website users’ browsers and devices and/or transmitted to the Third Parties along
16 with user data.


17 40. In particular, when users clicked or selected the “here” link, then adjusted all
18 available settings on the Your Choices window to opt out of, decline, or reject non-required
19 cookies, Defendant nonetheless continued to cause the Third Parties’ cookies, including
20 Functional and Advertising cookies to be placed on users’ devices and/or transmitted to the Third
21 Parties along with user data, causing them to collect user data in real time that discloses Website
22 visitors’ Private Communications, including browsing history, visit history, website interactions,
23 user input data, demographic information, interests and preferences, shopping behaviors, device
24 information, referring URLs, session information, user identifiers, and/or geolocation data. In
25 other words, even when consumers like Plaintiffs tried to protect their privacy by opting out of
26 or rejecting cookies, Defendant failed to prevent cookies from being transmitted to Third Parties,
27 causing them to track user behavior and communications.
28

← → ↻ <https://www.myfitnesspal.com/account/create/welcome>

Welcome to
myfitnesspal



Ready for some wins?
Start tracking, it's easy!



Elements Console Sources **Network** Performance Memory Application Set

Filter ☐ Invert ☐ Hide data URLs ☐ Hide extension URLs **All** Fetch/XHR

☒ 3rd-party requests
☐ Big request rows
☐ Overview

Name	Method	Status	Domain	Cookies
tr?id=272497224643685&ev=PageVi...	GET	200	www.facebook.com	7
trigger?id=272497224643685&ev=Su...	GET	200	www.facebook.com	7
tr?id=272497224643685&ev=Subscri...	GET	200	www.facebook.com	7
anchor?ar=1&k=6Ldo3qAhAAAAIAZy...	GET	200	www.google.com	6
webworker.js?hl=en&v=Hq4JZivTyQ7G...	GET	200	www.google.com	6
Cuj_kDox7kQB15k15ZfnF8OUB-ufBv...	GET	200	www.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	204	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	204	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	204	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	204	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	204	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	302	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	204	analytics.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	204	analytics.google.com	6
enterprise.js?render=6Ldo3qAhAAAA...	GET	200	www.google.com	6
collect?v=2&tid=G-HL1EGFN51C>m...	POST	204	analytics.google.com	6
anchor?ar=1&k=6Ldo3qAhAAAAIAZy...	GET	200	www.google.com	6
391609723?random=1711253331478&...	GET	200	td.doubleclick.net	3
391609723?random=1711253331478&...	GET	200	googleads.g.doubleclick.net	3
up?adv=7zokif7&ref=https%3A%2F%2...	GET	200	insight.adsrvr.org	3

Two screenshots of a web browser showing the myfitnesspal.com account creation page. The left screenshot shows the 'Welcome to myfitnesspal' page with a protein bar chart and a 'Ready for some wins? Start tracking, it's easy!' message. The right screenshot shows the 'Network' tab of Chrome Developer Tools, displaying a list of HTTP requests to various domains including amazon-adsystem.com, google-analytics.com, and analytics.tiktok.com.

42. The screenshots above show the “Network” tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user’s browser and various third-party websites while the user visited and interacted with Defendant’s Website at <https://www.myfitnesspal.com>. The screenshots depict only network traffic occurring *after* the user opted out of, declined, or rejected all cookies using the Your Choices window. As shown

1 above, despite the user's declination or rejection of all cookies, the user's interactions with the
2 Website resulted in the user's browser making a large number of GET and POST HTTP requests
3 to third party web domains like www.google.com; www.facebook.com; analytics.tiktok.com;
4 insight.adsrvr.org; and others. As further shown in the right-hand column of the screenshots, the
5 user's browser sent cookies along with those HTTP requests to the third parties. These
6 screenshots demonstrate that the Website caused third-party cookie data and users' Private
7 Communications to be transmitted to Third Parties, even after consumers declined or rejected all
8 such non-required cookies and tracking technologies by clicking or selecting the "here" link and
9 adjusting settings in the Your Choices window to decline or reject all non-required cookies,
10 including Functional and Advertising cookies. All of these network calls are made to the Third
11 Parties without the user's knowledge, and despite the user's rejection of all cookies.

12 43. Plaintiffs' and other Website users' Private Communications, including their
13 browsing history, visit history, website interactions, user input data, demographic information,
14 interests and preferences, shopping behaviors, device information, referring URLs, session
15 information, user identifiers, and/or geolocation data, were surreptitiously obtained by the Third
16 Parties via these cookies.

17 44. As users interact with the Website, even after clicking or selecting the "here" link,
18 then adjusting all available settings in the Your Choices window, thereby opting out of,
19 declining, or rejecting the use of cookies and similar technologies for analytics and
20 advertisements, as well as the sale or sharing of the user's personal information with third parties
21 for such functions, or other purposes, more data regarding users' behavior and communications
22 are sent to third parties, alongside the cookie data. The third-party cookies that Defendant
23 wrongfully allows to be stored on users' devices and browsers, and to be transmitted to the Third
24 Parties, cause the Third Parties to track and collect data on users' behaviors and communications,
25 including Private Communications, on the Website. Because third-party cookies cause Third
26 Parties to track users' behavior across the Internet and across time, user data can be correlated
27 and combined with other data sets to compile comprehensive user profiles that reflect
28

consumers' behavior, preferences, and demographics (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes). These Third Parties monetize user profiles for advertising, sales, and marketing purposes to generate revenue and target advertising to Internet users. Advertisers can gain deep understanding of users' behavioral traits and characteristics and target those users with advertisements tailored to their consumer profiles and audience segments.

45. The Third-Party code that the Website causes to be loaded and executed by the user's browser becomes a wiretap when it is executed because it causes the Third Parties—separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. When the Third Parties use their respective wiretaps on Website users' Private Communications, the wiretaps are not like tape recorders or “tools” used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

C. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Website.

1. Facebook Cookies

46. Defendant causes third party cookies to be transmitted to and from Website users' browsers and devices to and from the facebook.com domain, even after users elect to opt out of, decline, or reject all non-required cookies (including Functional and Advertising cookies). This domain is associated with Meta's digital advertising and analytics platform that collects user information via cookies to assist Meta in performing data collection, behavioral analysis, user retargeting, and analytics.² Meta serves targeted ads to web users across Meta's ad network, which spans millions of websites and apps.

47. The facebook.com cookies help Meta track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide

² <https://www.facebook.com/privacy/policies/cookies/>.

analytic metrics that advertisers use to measure ad campaign performance. For example, data is sent to Meta via the Facebook domain when the user enters data about their weight loss goal, such as in the following instance:



myfitnesspal

In the past, what have been your barriers to losing weight?
Select all that apply.

- Lack of time
- The regimen was too hard to follow
- Did not enjoy the food
- Difficult to make food choices
- Social eating and events
- Food cravings**
- Lack of progress

48. Here, the user has selected the “Food cravings” button, and in response, the following data is sent to Facebook:

Request	Header	Query	Body	Cookies	Raw	+
	Key		Value			
	id		272497224643685			
	ev		SubscribedButtonClick			
	dl		https%3A%2F%2Fwww.myfitnesspal.com%2Faccount%2Fcreate%2Fgoals%2Flose-weight%2Foptions			
	rl					
	if		false			
	ts		1711253552826			
	cd[buttonFeatures]		%7B"classList"%3A"MuiButtonBase-root%20MuiToggleButton-root%20MuiToggleButton-fullWidth%20MuiToggleButton-sizeMedium%20MuiToggleButton-standard%20MuiToggleButtonGroup-grouped%20MuiToggleButtonGroup-groupedVertical%20css-1ufxe7r"%2C"destination"%3A"https%3A%2F%2Fwww.myfitnesspal.com%2Faccount%2Fcreate%2Fgoals%2Flose-weight%2Foptions"%2C"id"%3A""%2C"imageUrl"%3A""%2C"innerText"%3A"Food%20cravings"%2C"numChildButtons"%3A0%2C>tag"%3A"button"%2C"type"%3A"button"%2C"name"%3A""%2C"value"%3A"food_cravings Lose"%7D			
	cd[buttonText]		Food%20cravings			
	cd[formFeatures]		%5B%7B"id"%3A""%2C"name"%3A""%2C>tag"%3A"button"%7D%2C%7B"id"%3A""%2C"name"%3A""%2C>tag"%3A"button"%7D%2C%7B"id"%3A""%2C"name"%3A""%2C>tag"%3A"button"%7D%2C%7B"id"%3A""%2C"name"%3A""%2C>tag"%3A"button"%7D%2C%7B"id"%3A""%2C"name"%3A""%2C>tag"%3A"button"%7D%2C%7B"id"%3A""%2C"name"%3A""%2C>tag"%3A"button"%7D%5D			
	cd[pageFeatures]		%7B"title"%3A"Create%20Your%20Free%20Account%20%7C%20MyFitnessPal"%7D			
	cd[parameters]		%5B%5D			
	sw		2240			
	sh		1260			
	v		2.9.150			
	r		stable			
	ec		16			
	o		4126			
	fbp		fb.1.1711253163792.1395291479			
	cs_est		true			
	ler		empty			
	cdl		API_unavailable			
	it		1711253331445			
	coo		false			
	es		automatic			
	tm		3			
	rqm		GET			

49. The “ev” parameter above tells Meta that the user clicked on a button, whereas the “cd[buttonText]” parameter tells Meta that the button’s text was “Food cravings.” Along with this data, cookie data is sent to Meta via the Facebook domain:

Key	Value
sb	FsT8ZfN5LvSnuDaNI8RhtnOd
datr	FsT8Zf1RzKc9J_QW2sezxlGM
ps_n	0
locale	en_US
c_user	1345507951
xs	41%3Atd5e- MLmwVuOgg%3A2%3A1711064122%3A-1%3A2633%3A %3AAcWhZCo6gSmAwYXmyyPVJDF8ddxrQxYRRFeflg0JdA
fr	1i609O136SvV207N0.AWVY1xt- IbUx8LZsl-3VgePZyAc.BI_1Ja..AAA.0.0.BI_1Ja.AWVCfET1IX s

50. The “c_user” cookie shown above causes Facebook to identify a specific user when they are logged in to their account. The “c_user” cookie stores a user’s unique ID, which is associated with their Facebook profile. This ID causes Facebook to track user interactions on its platform and across sites that use Facebook plugins, such as adding items to a cart, clicking “Like” buttons, or engaging with comment sections. When combined with other data sent to the Facebook domain, this cookie allows Meta to track users’ browsing activities. Facebook uses this data for various purposes, such as personalizing content, enhancing ad targeting accuracy, and refining its user experience.

51. In particular, by identifying users who have shown interest in certain products or content, the facebook.com cookies cause Meta’s advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Meta’s ad network.³ These cookies allow Meta to collect data on how users interact with websites, regardless of whether they have a Facebook account or are logged in.⁴

³ *Id.*; <https://allaboutcookies.org/what-data-does-facebook-collect>.

⁴ <https://allaboutcookies.org/what-data-does-facebook-collect>.

52. The facebook.com cookies allow Meta to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses)—including whether a user is located in California.⁵

53. Meta utilizes the data collected through the facebook.com cookies for its own purposes, including by using the data to tailor content and target advertisements to users. This includes practices such as (i) **Ad Targeting and Retargeting**, in which Meta uses the facebook.com cookie to track users' online behavior across different sites, building a profile based on their browsing habits, purchases, and interactions. This profile causes Facebook to deliver highly targeted ads within the Facebook ecosystem and on other sites that are part of Facebook's Audience Network; (ii) **Conversion Tracking**, in which Meta uses the facebook.com cookie to enable business partners to track specific actions users take after viewing or clicking on a Facebook ad, such as making a purchase or signing up for a newsletter; (iii) **Audience Insights and Analytics**, in which Meta uses the facebook.com cookie to provide data to businesses on user demographics, interests, and behaviors across their sites and apps; and (iv) **Cross-Device and Cross-Platform Tracking**, in which Meta uses the facebook.com cookie to support tracking users across devices and platforms, so that ads are targeted consistently regardless of the device a user is on. This ensures that advertisers can follow users across devices.

2. Google Cookies

54. Defendant also causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users opt out of, decline, or reject all non-required cookies (including Functional and Advertising cookies) to and from the www.google.com, doubleclick.net, analytics.google.com, and www.google-analytics.com domains. Each of these domains is associated with Google LLC's digital advertising and analytics platform that

⁵ *Id.*

collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.⁶ Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's DoubleClick cookies.⁷ Google's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. Further, by identifying users who have shown interest in certain products or content, Google's cookies cause its advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Google's ad network.⁸

55. Specifically, Google sends cookies when a web user visits a webpage that shows Google Marketing Platform advertising products and/or Google Ad Manager ads.⁹ "Pages with Google Marketing Platform advertising products or Google Ad Manager ads include ad tags that instruct browsers to request ad content from [Google's] servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google Marketing Platform advertising products or Google Ad Manager ads for this to happen; it just needs to include Google Marketing Platform advertising products or Google Ad Manager ad tags, which might load a click tracker or impression pixel instead." *Id.* As Google explains, "Google Marketing Platform advertising products and Google Ad Manager send a cookie to the browser after any impression, click, or other activity that results in a call to our servers." *Id.*

⁶ See Our advertising and measurement cookies (available at <https://business.safety.google/adscookies/>).

⁷ See, e.g. <https://www.ghostery.com/whotracksme/trackers/doubleclick>.

⁸ See, e.g. About cross-channel remarketing in Search Ads 360 (available at <https://support.google.com/searchads/answer/7189623?hl=en>); About dynamic remarketing for retail (available at <https://support.google.com/google-ads/answer/6099158?hl=en&sjid=1196213575075458908-NC>).

⁹ See How Google Marketing Platform advertising products and Google Ad Manager use cookies (available at <https://support.google.com/searchads/answer/2839090?hl=en&sjid=1196213575075458908-NC>); see also Cookies and user identification (available at <https://developers.google.com/tag-platform/security/concepts/cookies>).

56. Google also uses cookies in performing analytical functions. As Google explains, “Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es].”¹⁰ “To measure a website ... [one] add[s] a small piece of JavaScript measurement code to each page on [a] site.” *Id.* Then, “[e]very time a user visits a webpage, the tracking code will collect ... information about how that user interacted with the page.” *Id.* Google Analytics enables website owners to “measure when someone loads a page, clicks a link, [] makes a purchase;” “completes a purchase;” “searches [] website or app;” “select content on [] website or app;” “views an item;” and “views their shopping cart.”¹¹

57. Google’s cookies allow it to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data.¹²

58. For example, the Google software code that Defendant causes to be stored on and executed by the Website user’s device causes the following data to be sent to Google’s advertising domain, at td.doubleclick.net:

¹⁰ How Google Analytics Works (available at <https://support.google.com/analytics/answer/12159447?hl=en>).

¹¹ Set up events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>); and Recommended events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>).

¹² See About the Google Tag (available at <https://support.google.com/searchads/answer/7550511?hl=en>); How Floodlight Recognizes Users (available at <https://support.google.com/searchads/answer/2903014?hl=en>); How Google Ads tracks website conversions (available at <https://support.google.com/google-ads/answer/7521212>); Google Ads Help, Cookie: Definition (available at <https://support.google.com/google-ads/answer/2407785?hl=en>); About demographic targeting in Google Ads (available at https://support.google.com/searchads/answer/7298581?hl=en&sjid=1196213575075458908-NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1); How Google Analytics Works (<https://support.google.com/analytics/answer/12159447>); Set up events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>); and Recommended events (available at <https://support.google.com/analytics/answer/9267735>).

Request	Header	Query	Body	Cookies	Raw	+
Key	Value					
random	1711253331478					
cv	11					
fst	1711253331478					
fmt	3					
bg	ffffff					
guid	ON					
async	1					
gtm	45be43k0v870235405z8863704985za201					
gcd	13l3l3l3l1					
dma	0					
u_w	2240					
u_h	1260					
url	https://www.myfitnesspal.com/?_branch_match_id=1299969674994722193&utm_medium=webtoapp&_branch_referrer=H4slAAAAAAAAA8soKSkottLXz61MyyzJSy0uLkjM0UssKNDLycL1i80DnQN9HbPSfRIAgDP%2B0nIKQAAAA%3D%3D					
hn	www.googleadservices.com					
frm	0					
tiba	Calorie Tracker & BMR Calculator to Reach Your Goals MyFitnessPal					
npa	0					
us_privacy	error					
pscdl	noapi					
auid	819799128.1711253164					
uaa	arm					
uab	64					
uafvl	Google%20Chrome;123.0.6312.59 Not%3AA-Brand;8.0.0.0 Chromium;123.0.6312.59					
uamb	0					
uam						
uap	macOS					
uapv	14.4.0					
uaw	0					
fledge	1					

59. The “npa” parameter refers to “Non-Personalized Ads.” When npa is set to 1, it indicates non-personalized ads preference is enabled. Here, npa is set to 0, indicating that standard (personalized) ads are enabled. The “uap” and “uapv” parameters tell Google the operating system and version the consumer is using, while the “uafvl” parameter discloses the user’s browser.

60. Along with this data, the following type of cookie data is sent to Google:

Request	Header	Query	Body	Cookies	Raw	+
Key	Value					
ar_debug	1					
DSID	AOUHqapYImNCD0WHGrGp3VHq8PoFQqhzYHPxrMaVZ72 iSwoEokwc7yBx8nxEX72WYJWc_gQ8yQbQNGPSgj5dJS5 YIfPJSIhnf5uH- bTBJrnDn1wBQgP9z9NUr1a9Nv6UyHXIB4FpCinOp2yuhx w- WqgFYpdOedSLrMkqEBnX1wW1KE_R1wDFijp0MGAf6eylh skRzdCcOvVxPlwOazuwLr2L9MrtI5RLUIRz0g02fVsw__f6O G1hCJvJ57VJOEyn73JgrXGnK1zO2viE3ScQtt_GGNk6Ozh Qw_QRjicrLx9UC6Tm8H-XdlU					
IDE	AHWqTUmxBZTe_eHtG8b-88bJx0wdjFaWPxXlaabdH0HyZ a76GDGdqNFAX_DVxKn68rY					

61. Google uses the “DSID” cookie to “identify a signed-in user on non-Google sites.”¹³ The “IDE” cookie is used “to personalize the ads [users] see” and “to show Google ads on non-Google sites.”¹⁴

62. Finally, the data sent to Google contains the user’s user-agent and IP address—which can be used to determine a user’s geolocation, including whether they are located in California.

63. Because Google’s cookies operate across multiple sites (i.e., cross-site tracking), the cookie causes Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google’s advertising platform aggregates user data to create consumer profiles containing detailed information about a consumer’s behavior, preferences, and demographics and audience segments based on shared traits (such as females, Millennials, Californians, etc.), and to perform targeted advertising and marketing analytics.

64. Thus, the Google cookies used on the Website cause Google to track Website users’ interactions with advertisements to help advertisers understand how users engage with ads across different websites. Further, the user data collected through the cookie enables the delivery

¹³ <https://policies.google.com/technologies/cookies?hl=en-US>.

¹⁴ *Id.*

of personalized ads based on user interests and behaviors. For instance, if a user frequently visits travel-related websites, Google will show her more travel-related advertisements. Further, the collected data is used to generate reports for advertisers, helping them assess the performance of their ad campaigns and make data-driven decisions (such as renaming their products). Further, Google’s advertising platform enables advertisers to retarget marketing, which Google explains allows advertisers to “show previous visitors ads based on products or services they viewed on your website. With messages tailored to your audience, dynamic remarketing helps you build leads and sales by bringing previous visitors back to your website to complete what they started.”¹⁵

65. Further, in its “Shared Data Under Measurement Controller-Controller Data Protection Terms,” Google states: “Google can access and analyze the Analytics data customers share with us to better understand online behavior and trends, and improve our products and services—for example, to improve Google search results, detect and remove invalid advertising traffic in Google Ads, and test algorithms and build models that power services like Google Analytics Intelligence that apply machine-learning to surface suggestions and insights for customers based on their analytics data and like Google Ads that applies broad models to improve ads personalization and relevance. These capabilities are critical to the value of the products we deliver to customers today.”¹⁶ Thus, Google can have the capability to use the data it collects for understanding online behavior and trends, machine learning, and improving its own products and services.

3. TikTok Cookies

66. Defendant also causes third party cookies to be transmitted to and from Website users’ browsers and devices, even after users elect to opt out of, decline, or reject all non-required cookies, to and from the [analytics.tiktok.com](https://support.google.com/analytics/answer/9024351) domain. This domain is associated with TikTok for Business, a suite of tools offered by TikTok, a social media platform owned by

¹⁵ Dynamic remarketing for web setup guide (available at <https://support.google.com/google-ads/answer/6077124>).

¹⁶ Shared Data Under Measurement Controller-Controller Data Protection Terms (available at <https://support.google.com/analytics/answer/9024351>).

ByteDance Ltd., known for short-form video sharing.¹⁷ The TikTok platform is used to create and share videos, and it utilizes cookies for various purposes including assisting brands and marketers to create, manage, and optimize ad campaigns on the platform.¹⁸

67. TikTok utilizes analytics.tiktok.com cookies to collect data on user interactions with websites that have integrated TikTok’s tracking technologies (such as the Website). These cookies are used to “measure and improve the performance of your advertising campaigns and to personalize the user’s experience (including ads) on TikTok.”¹⁹ TikTok further explains that it uses cookies to “match events with people who engage with your content on TikTok. Matched events are used to improve measurement and optimize ad campaigns. They can also contribute to building your retargeting and engagement audiences.” *Id.* These cookies cause TikTok to recognize and track users across different sessions and domains (i.e., cross-site tracking) and to collect and synchronize user data to observe and evaluate TikTok user behavior.

68. These cookies cause TikTok to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, including *email addresses and phone numbers*; (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) session information, (x) user identifiers, and (xi) geolocation data in the form of the IP address.²⁰

69. For example, the TikTok software code that Defendant causes to be stored on and executed by the Website user’s device causes the following type of data to be sent to TikTok’s domain, at analytics.tiktok.com:

¹⁷ See Our advertising and measurement cookies (available at <https://business.safety.google/adscookies/>).

¹⁸ See, e.g., TikTok for Business (<https://ads.tiktok.com/business/en-US/products/ads>; and <https://ads.tiktok.com/business/en-US/products/measurement>); TikTok Business Help Center; Using Cookies with TikTok Pixel (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

¹⁹ TikTok Business Help Center; Using Cookies with TikTok Pixel (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

²⁰ *Id.*; see also TikTok for Business: Enhance Data Postback with the TikTok Pixel (<https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel?lang=en>); TikTok for Business: Advanced Matching for Web (available at <https://ads.tiktok.com/help/article/advanced-matching-web?redirected=1>); TikTok for Business: About TikTok Pixel (available at <https://ads.tiktok.com/help/article/tiktok-pixel?lang=en>).

Request Header Query Body Cookies Raw +		Tree View
Key	Value	
Root	Object(10 items)	
> signal_diagnostic_labels	Object(6 items)	
action	Metadata	
message_id	messageId-1711253338961-6676689735430	
> context	Object(11 items)	
> device	Object(1 items)	
index	7	
> library	Object(2 items)	
variation_id	test_2_single_track_idle	
> pixel	Object(3 items)	
runtime	1	
codes	CF8MB03C77UEUGLDMSM0	
code	CF8MB03C77UEUGLDMSM0	
> ad	Object(2 items)	
sdk_env	external	
jsb_status	2	
session_id	d4fbf8d5-e993-11ee-8ce1-c211db8d982a::Jj_7D9ccb-3hH...	
pageview_id	pageId-1711253338761-3753820909446	
userAgent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit...	
> page	Object(2 items)	
url	https://www.myfitnesspal.com/account/create/input-name	
referrer	https://www.myfitnesspal.com/account/create/welcome	
> user	Object(1 items)	
anonymous_id	dtJYnsRTNOy8grgij9Eppl9ChX0	
event_id		
is_onsite	false	
properties	Object(0 items)	
timestamp	2024-03-24T04:08:58.961Z	
> auto_collected_properties	Object(2 items)	
_inspection	Object(0 items)	

70. The data includes the “session_id,” which is a unique identifier generated by TikTok to track a user’s activity. This allows TikTok to correlate the user’s behavior from a browsing session, including page views and conversions, to a particular user to enhance advertising measurement, attribution, and targeting.²¹

71. Along with this data, Defendant causes cookie data to be sent to TikTok, such as the following:

POST	200	https://analytics.tiktok.com/api/v2/pixel/act
Request Header Query Body Cookies Raw +		
Key	Value	
_ttp	2e1FPiDB5ocR8LuQjvXrakaoqM0	

²¹ See, e.g., How to get TikTok session id? (available at <https://gbtimes.com/how-to-get-tiktok-session-id/>).

72. According to TikTok’s documentation, the “_ttp” cookie is one of the company’s advertising cookies, the purpose of which is “[t]o measure and improve the performance of your advertising campaigns and to personalize the user’s experience (including ads) on TikTok.”²²

73. Finally, the data sent to TikTok includes the user’s user-agent and IP address, which can, among other things, allow Facebook to know that a user is located in California.

74. By collecting this user data, TikTok performs user behavior tracking, i.e., monitoring user actions like page views, clicks, and interactions to understand user engagement; advertising optimization, i.e., gathering data to enhance the relevance and effectiveness of TikTok advertising campaigns; and performance measurement (i.e., assessing the success of marketing efforts by analyze user responses to ads and content).²³

75. Further, TikTok’s Automatic Advanced Matching feature functions as follows: “When a visitor lands on your website and inputs customer information during registration, sign-in, contact, or checkout on a website where you installed your pixel, Automatic Advanced Matching will capture information from those fields. ...TikTok will use hashed information to link event information to people on TikTok. Tiktok may use matched events to better attribute events to TikTok ads, optimize advertisers’ future campaigns, and depending on advertisers’ and users’ settings, TikTok may also add people to advertisers’ retargeting or engagement audiences.”²⁴

4. Additional Third-Party Cookies

76. Defendant also causes third party cookies to be transmitted to and from Website users’ browsers and devices, even after users elect to opt out of, decline, or reject all non-required cookies, to and from other domains, including amazon-adsystem.com and insight.adsrvr.org.

²² See *TikTok for Business: Using Cookies with TikTok Pixel* (available at <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>).

²³ *Id.*

²⁴ TikTok for Business: How to set up Automatic Advanced Matching (available at <https://ads.tiktok.com/help/article/how-to-set-up-automatic-advanced-matching?lang=en>).

77. The c.amazon-adsystem.com domain is associated with Amazon's advertising services. Amazon utilizes cookies to collect data on user interactions with websites (including browsing behavior and preferences) to perform advertising and personalization functions, i.e., to assist Amazon in delivering advertisements tailored to user interests. Further, the cookies perform analytics functions to enable Amazon to measure and analyze the performance of its services and to ensure that ads are effective and relevant.

78. The insight.adsrvr.org domain is associated with The Trade Desk, Inc., a digital advertising company that offers a cloud-based ad-buying platform that enables businesses to plan, manage, optimize, and measure data-driven digital advertising campaigns.²⁵ The Trade Desk uses insight.adsrvr.org cookies to collect data on users such as their geographic locations, the type of device users are using, and users' interests as inferred from their web browsing or app usage activity."²⁶ This data helps The Trade Desk personalize ad content and track users across the internet.²⁷

79. These cookies allow these Third Parties to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) demographic information, (v) interests and preferences, (vi) shopping behaviors, (vii) device information, (viii) referring URLs, (ix) session information, (x) user identifiers, and/or (xi) geolocation data.

D. The Private Communications Collected are Valuable.

80. As part of its regular course of business, Defendant targets California consumers by causing the Third Parties to extract, collect, maintain, distribute, and exploit for Defendant's and the Third Parties' profit, all of the Private Communications transferred by the cookies which Defendant causes to be placed on Plaintiffs' and other California Website users' devices without their knowledge or consent. Defendant knew the location of consumers like Plaintiffs and the

²⁵ See The Trade Desk, Inc. 2023 Form 10-K (filed February, 15 2024).

²⁶ *Id.*

²⁷ *Id.*

1 Class members either prior to or shortly after causing the Third Parties to use cookies on their
2 devices.

3 81. The Private Communications that the Third Parties track and collect by way of
4 the cookies on the Website are valuable to Defendant as well as the Third Parties. Defendant can
5 use the data to create and analyze the performance of marketing campaigns, website design,
6 product placement, and target specific users or groups of users for advertisements. For instance,
7 if Defendant wanted to market certain features of its fitness application, or related services, to
8 consumers in California, Defendant could use the data collected by the Third Parties to monitor
9 the location of users who visit webpages related to specific products, then advertise similar
10 products or services to those particular users when they visit other webpages. The third-party
11 cookies also enable Defendant to target online advertisements to users when they visit *other*
12 websites, even those completely unrelated to Defendant and its products or services.

13 82. Data about users' browsing history enables Defendant to spot patterns in users'
14 behavior on the Website and their interests in, among other things, Defendant's fitness
15 application and specific features or services associated with the application. On a broader scale,
16 it enables Defendant to gain an understanding of trends happening across its brands and across
17 the nutrition and fitness application and services market. All of this helps Defendant further
18 monetize its Website and application and maximize revenue by collecting and analyzing user
19 data.

20 83. The value of the Private Communications tracked and collected by the Third
21 Parties using cookies on the Website can be quantified. Legal scholars observe that "[p]ersonal
22 information is an important currency in the new millennium."²⁸ Indeed, "[t]he monetary value
23 of personal data is large and still growing, and corporate America is moving quickly to profit
24 from the trend." *Id.* "Companies view this information as a corporate asset and have invested
25 heavily in software that facilitates the collection of consumer information." *Id.*

26
27
28 ²⁸ See Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004).

89. Consistent with his typical practice in opting out of, rejecting, or otherwise declining the placement or use of cookies and tracking technologies, Plaintiff Shah selected and clicked the “here” link to opt out of the use and placement of cookies. In doing so, Plaintiff Shah was then directed to the Your Choices window, which further represented that users could “choose whether this site may use Functional and/or Advertising cookies[.]” Accordingly, Plaintiff Shah adjusted all available settings in the Your Choices window to the “[opt] OUT” position, indicating his choice/agreement to reject all cookies, including Functional and Advertising cookies, except the “Required Cookies” that Plaintiff Shah was unable to reject. Plaintiff Shah then clicked or selected the “Submit Preferences” button and continued to browse the Website.

90. Plaintiff Shah believed that selecting the “here” link on the popup cookie consent banner and adjusting all available settings in the Your Choices window, would allow him to opt out of, decline, and/or reject all non-required cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of tracking data to third-party advertising networks and analytics services for the purposes of providing personalized content, advertising, and analytics services).

91. In selecting the “here” link and adjusting all available settings to opt out of, decline, or reject cookies on the Your Choices window, Plaintiff Shah gave Defendant notice that he did not consent to the use or placement of cookies and tracking technologies while browsing the Website, other than those “Required” for the operation of the Website. Further, Plaintiff Shah specifically opted out of, declined, or otherwise rejected, based on Defendant’s representations, those cookies used “for analytics...and to personalize content and ads” and share information with third parties. In reliance on these representations and promises, only then did Plaintiff Shah continue browsing the Website.

92. Even before the popup cookie consent banner appeared on the screen, Defendant nonetheless caused cookies and tracking technologies, including those used for personalized content, advertising, and analytics, to be placed on Plaintiff Shah’s device and/or transmitted to

1 the Third Parties along with user data, without Plaintiff Shah's knowledge. Accordingly, the
2 representations found on the popup cookie consent banner and Your Choices window, that
3 Plaintiff Shah could "opt out of the use of certain cookies" and "choose whether this site may
4 use Functional and/or Advertising cookies" while he browsed the Website, were false. Contrary
5 to what Defendant made Plaintiff Shah believe, he did not have a choice about whether third-
6 party cookies would be placed on his device and/or transmitted to the Third Parties along with
7 his user data; rather, Defendant had already caused that to happen.

8 93. Then, as Plaintiff Shah continued to browse the Website in reliance on the
9 promises Defendant made in the cookie consent banner and Your Choices window, and, despite
10 Plaintiff Shah's clear rejection of the use and/or placement of such cookies and tracking
11 technologies, Defendant nonetheless continued to cause the placement and/or transmission of
12 cookies along with user data, including those involved in providing personalized content,
13 advertising, and analytics from the Third Parties on his device. In doing so, Defendant permitted
14 the Third Parties to track and collect Plaintiff Shah's Private Communications as Plaintiff Shah
15 browsed the Website.

16 94. Defendant's representations that consumers could "opt out of", decline, or reject
17 all cookies, including Functional and Advertising cookies, other than those required for the
18 operation of the Website, while Plaintiff Shah and users browsed the Website, or at least opt out
19 of those cookies involved in providing personalized content, analytics, and advertising were
20 untrue. Had Plaintiff Shah known this fact, he would not have used the Website. Moreover,
21 Plaintiff Shah reviewed the popup cookie consent banner, Your Choices window, and Privacy
22 Policy prior to using the Website. Had Defendant disclosed that it would continue to cause
23 cookies and tracking technologies to be stored on consumers' devices, even after they choose to
24 opt out of, decline, or otherwise reject all non-required cookies, Plaintiff Shah would have
25 noticed it and would not have used the Website or, at a minimum, he would have interacted with
26 the Website differently.

1 95. Plaintiff Shah continues to desire to browse content featured on the Website.
2 Plaintiff Shah would like to browse websites that do not misrepresent that users can opt out of,
3 decline, or otherwise reject all non-required cookies and tracking technologies. If the Website
4 were programmed to honor users' requests to opt out of, decline, or otherwise reject all non-
5 required cookies and tracking technologies, Plaintiff Shah would likely browse the Website
6 again in the future, but will not do so until then. Plaintiff Shah regularly visits websites that
7 feature content similar to that of the Website. Because Plaintiff Shah does not know how the
8 Website is programmed, which can change over time, and because he does not have the technical
9 knowledge necessary to test whether the Website honors users' requests to opt out of, decline,
10 or reject all non-required cookies and tracking technologies, Plaintiff Shah will be unable to rely
11 on Defendant's representations when browsing the Website in the future absent an injunction
12 that prohibits Defendant from making misrepresentations on the Website. The only way to
13 determine what network traffic is sent to third parties when visiting a website is to use a
14 specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed
15 for use by "developers" (i.e., software developers), whose specialized training enables them to
16 analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to
17 whom. Plaintiff Shah is not a software developer and he has not received training with respect
18 to HTTP network calls.

19 **B. Plaintiff Christine Wiley**

20 96. Plaintiff Wiley visited the Website to seek information about MyFitnessPal's
21 products or services, while located in California, on one or more occasions during the last four
22 years.

23 97. Plaintiff Wiley's visits to the Website were consistent with a typical Website
24 user's visits seeking information about MyFitnessPal's products or services. Specifically,
25 Plaintiff Wiley is not a consumer advocate, a "tester," or a compliance auditor that visited the
26 Website to test or evaluate Defendant's privacy practices.
27
28

1 98. When Plaintiff Wiley visited the Website, the Website immediately detected that
2 she was a visitor in California and presented her with Defendant’s popup cookie consent banner,
3 which provided the option to opt out of certain cookies by clicking the “here” link. Plaintiff
4 Wiley viewed Defendant’s representation on the popup cookie consent banner that, “We use first
5 and third party cookies to make our site work (Required Cookies), for analytics (Functional
6 Cookies), and to personalize content and ads (Advertising Cookies). You may opt out of the use
7 of certain cookies here.” Plaintiff Wiley saw that the word “here” was a link that she could click
8 or select.

9 99. Consistent with her typical practice in opting out of, rejecting, or otherwise
10 declining the placement or use of cookies and tracking technologies, Plaintiff Wiley selected and
11 clicked the “here” link to opt out of the use and placement of cookies. In doing so, Plaintiff Wiley
12 was then directed to the Your Choices window, which further represented that users could
13 “choose whether this site may use Functional and/or Advertising cookies[.]” Accordingly,
14 Plaintiff Wiley adjusted all available settings in the Your Choices window to the “[opt] OUT”
15 position, indicating her choice/agreement to reject all cookies, including Functional and
16 Advertising cookies, except the “Required Cookies” that Plaintiff Wiley was unable to reject.
17 Plaintiff Wiley then clicked or selected the “Submit Preferences” button and continued to browse
18 the Website.

19 100. Plaintiff Wiley believed that selecting the “here” link on the popup cookie consent
20 banner and adjusting all available settings in the Your Choices window, would allow her to opt
21 out of, decline, and/or reject all non-required cookies and other tracking technologies (inclusive
22 of those cookies that cause the disclosure of tracking data to third-party advertising networks
23 and analytics services for the purposes of providing personalized content, advertising, and
24 analytics services).

25 101. In selecting the “here” link and adjusting all available settings to opt out of,
26 decline, or reject cookies on the Your Choices window, Plaintiff Wiley gave Defendant notice
27 that she did not consent to the use or placement of cookies and tracking technologies while
28

1 browsing the Website, other than those “Required” for the operation of the Website. Further,
2 Plaintiff Wiley specifically opted out of, declined, or otherwise rejected, based on Defendant’s
3 representations, those cookies used “for analytics...and to personalize content and ads” and share
4 information with third parties. In reliance on these representations and promises, only then did
5 Plaintiff Wiley continue browsing the Website.

6 102. Even before the popup cookie consent banner appeared on the screen, Defendant
7 nonetheless caused cookies and tracking technologies, including those used for personalized
8 content, advertising, and analytics, to be placed on Plaintiff Wiley’s device and/or transmitted to
9 the Third Parties along with user data, without her knowledge. Accordingly, the representations
10 found on the popup cookie consent banner and Your Choices window, that Plaintiff Wiley could
11 “opt out of the use of certain cookies” and “choose whether this site may use Functional and/or
12 Advertising cookies” while she browsed the Website, were false. Contrary to what Defendant
13 made Plaintiff Wiley believe, she did not have a choice about whether third-party cookies would
14 be placed on her device and/or transmitted to the Third Parties along with her user data; rather,
15 Defendant had already caused that to happen.

16 103. Then, as Plaintiff Wiley continued to browse the Website in reliance on the
17 promises Defendant made in the cookie consent banner and Your Choices window, and, despite
18 Plaintiff Wiley’s clear rejection of the use and/or placement of such cookies and tracking
19 technologies, Defendant nonetheless continued to cause the placement and/or transmission of
20 cookies along with user data, including those involved in providing personalized content,
21 advertising, and analytics from the Third Parties on her device. In doing so, Defendant permitted
22 the Third Parties to track and collect Plaintiff Wiley’s Private Communications as she browsed
23 the Website.

24 104. Defendant’s representations that consumers could “opt out of”, decline, or reject
25 all cookies, including Functional and Advertising cookies, other than those required for the
26 operation of the Website, while Plaintiff Wiley and users browsed the Website, or at least opt
27 out of those cookies involved in providing personalized content, analytics, and advertising were
28

1 untrue. Had Plaintiff Wiley known this fact, she would not have used the Website. Moreover,
2 Plaintiff Wiley reviewed the popup cookie consent banner, Your Choices window, and Privacy
3 Policy prior to using the Website. Had Defendant disclosed that it would continue to cause
4 cookies and tracking technologies to be stored on consumers' devices, even after they choose to
5 opt out of, decline, or otherwise reject all non-required cookies, Plaintiff Wiley would have
6 noticed it and would not have used the Website or, at a minimum, she would have interacted
7 with the Website differently.

8 105. Plaintiff Wiley continues to desire to browse content featured on the Website.
9 Plaintiff Wiley would like to browse websites that do not misrepresent that users can opt out of,
10 decline, or otherwise reject all non-required cookies and tracking technologies. If the Website
11 were programmed to honor users' requests to opt out of, decline, or otherwise reject all non-
12 required cookies and tracking technologies, Plaintiff Wiley would likely browse the Website
13 again in the future, but will not do so until then. Plaintiff Wiley regularly visits websites that
14 feature content similar to that of the Website. Because Plaintiff Wiley does not know how the
15 Website is programmed, which can change over time, and because she does not have the
16 technical knowledge necessary to test whether the Website honors users' requests to opt out of,
17 decline, or reject all non-required cookies and tracking technologies, Plaintiff Wiley will be
18 unable to rely on Defendant's representations when browsing the Website in the future absent
19 an injunction that prohibits Defendant from making misrepresentations on the Website. The only
20 way to determine what network traffic is sent to third parties when visiting a website is to use a
21 specialized tool such as Chrome Developer Tools. As the name suggests, such tools are designed
22 for use by "developers" (i.e., software developers), whose specialized training enables them to
23 analyze the data underlying the HTTP traffic to determine what data, if any, is being sent to
24 whom. Plaintiff Wiley is not a software developer and she has not received training with respect
25 to HTTP network calls.

CLASS ALLEGATIONS

106. Plaintiffs bring this Class Action Complaint on behalf of themselves and a proposed class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure. Plaintiffs seek to represent the following group of similarly situated persons, defined as follows:

Class: All persons who, while in the State of California, browsed the Website after clicking the “here” link in the popup cookies consent banner and adjusting all available settings in the “Your Choices” window to opt out of, decline, or reject all non-required cookies, including Functional and Advertising cookies.

107. This action has been brought and may properly be maintained as a class action against Defendant because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

108. **Numerosity:** Plaintiffs do not know the exact size of the Class, but they estimate that it is composed of more than 100 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

109. **Common Questions Predominate:** This action involves common questions of law and fact to the Class because each class member’s claim derives from the same unlawful conduct that led them to believe that Defendant would not cause third-party cookies to be placed on their browsers and devices and/or transmitted to third parties along with user data, after Class members chose to opt out of, decline, or otherwise reject all non-required cookies and tracking technologies on the Website, nor would Defendant permit third parties to track and collect Class members’ Private Communications as Class members browsed the Website.

110. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class are:

a. Whether Defendant’s actions violate California laws invoked herein; and

1 b. Whether Plaintiffs and Class members are entitled to damages, restitution,
2 injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest and costs
3 of this suit.

4 111. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of
5 the Class because, among other things, Plaintiffs, like the other Class members, visited the
6 Website, opted out of, declined, or otherwise rejected non-required cookies, and had their
7 confidential Private Communications intercepted by the Third Parties.

8 112. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the
9 interests of all Class members because it is in their best interests to prosecute the claims alleged
10 herein to obtain full compensation due to him for the unfair and illegal conduct of which they
11 complain. Plaintiffs also have no interest in conflict with, or antagonistic to, the interests of Class
12 members. Plaintiffs have retained highly competent and experienced class action attorneys to
13 represent their interests and those of the Class. By prevailing on his claims, Plaintiffs will
14 establish Defendant's liability to all Class members. Plaintiffs and their counsel have the
15 necessary financial resources to adequately and vigorously litigate this class action, and Plaintiffs
16 and counsel are aware of their fiduciary responsibilities to the Class members and are determined
17 to diligently discharge those duties by vigorously seeking the maximum possible recovery for
18 Class members.
19

20 113. **Superiority:** There is no plain, speedy, or adequate remedy other than by
21 maintenance of this class action. The prosecution of individual remedies by members of the Class
22 will tend to establish inconsistent standards of conduct for Defendant and result in the
23 impairment of Class members' rights and the disposition of their interests through actions to
24 which they were not parties. Class action treatment will permit a large number of similarly
25 situated persons to prosecute their common claims in a single forum simultaneously, efficiently,
26 and without the unnecessary duplication of effort and expense that numerous individual actions
27 would engender. Furthermore, as the damages suffered by each individual member of the Class
28

may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

First Cause of Action: Invasion of Privacy

114. Plaintiffs reallege and incorporates the paragraphs of this Complaint as if set forth herein.

115. To plead an invasion of privacy claim, Plaintiffs must show an invasion of (i) a legally protected privacy interest; (ii) where Plaintiffs had a reasonable expectation of privacy in the circumstances; and (iii) conduct by Defendant constituting a serious invasion of privacy.

116. Defendant has intruded upon the following legally protected privacy interests of Plaintiffs and Class members: (i) the California Invasion of Privacy Act, as alleged herein; (ii) the California Constitution, which guarantees Californians the right to privacy; (iii) the California Wiretap Acts as alleged herein; (iv) Cal. Penal Code § 484(a), which prohibits the knowing theft or defrauding of property “by any false or fraudulent representation or pretense;” and (v) Plaintiffs’ and Class members’ Fourth Amendment right to privacy.

117. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as Defendant affirmatively promised users they could “opt out of the use of certain cookies” and “choose whether this site may use Functional and/or Advertising cookies” for “analytics...and to personalize content and ads[,]” among other purposes of the Functional and Advertising cookies, and related tracking technologies, as described in the consent banner and Your Choices window, and elsewhere, before users proceeded to browse the Website. Plaintiffs and other Class members directed their electronic devices to access the Website and, when presented with the popup cookies consent banner and Your Choices window on the Website, Plaintiffs and Class members opted out of, declined, or otherwise rejected all non-

1 required cookies and reasonably expected that his and their choice to opt out of, decline, or
2 otherwise reject such non-required cookies and tracking technologies would be honored. That is,
3 they reasonably believed that Defendant would not permit the Third Parties to store and send
4 cookies and/or use other such tracking technologies on their devices while they browsed the
5 Website. Plaintiffs and Class members also reasonably expected that, if they opted out of,
6 declined, or otherwise rejected such cookies and/or tracking technologies, Defendant would not
7 permit the Third Parties to track and collect Plaintiffs' and Class members' Private
8 Communications, including their browsing history, visit history, website interactions, user input
9 data, demographic information, interests and preferences, shopping behaviors, device
10 information, referring URLs, session information, user identifiers, and/or geolocation data, on
11 the Website.

12 118. Such information is "personal information" under California law, which defines
13 personal information as including "Internet or other electronic network activity information,"
14 such as "browsing history, search history, and information regarding a consumer's interaction
15 with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

16 119. Defendant, in violation of Plaintiffs' and other Class members' reasonable
17 expectation of privacy and without their consent, permits the Third Parties to use cookies and
18 other tracking technologies to collect, track, and compile users' Private Communications,
19 including their browsing history, visit history, website interactions, user input data, demographic
20 information, interests and preferences, shopping behaviors, device information, referring URLs,
21 session information, user identifiers, and/or geolocation data. The data that Defendant allowed
22 third parties to collect enables the Third Parties to (and the Third Parties actually do), *inter alia*,
23 create consumer profiles containing detailed information about a consumer's behavior,
24 preferences, and demographics; create audience segments based on shared traits (such as
25 millennials, tech enthusiasts, etc.); and perform targeted advertising and marketing analytics.
26 Further, the Third Parties share user data and/or the user profiles to unknown parties to further
27 their financial gain. The consumer profiles are and can be used to further invade Plaintiffs' and
28

1 users' privacy, by allowing third parties to learn intimate details of their lives, and target them
2 for advertising and other purposes, as described herein, thereby harming them through the
3 abrogation of their autonomy and their ability to control dissemination and use of information
4 about them.

5 120. Defendant's actions constituted a serious invasion of privacy in that it invaded a
6 zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and
7 violated criminal laws on wiretapping and invasion of privacy. These acts constitute an egregious
8 breach of social norms that is highly offensive.

9 121. Defendant's intrusion into Plaintiffs' privacy was also highly offensive to a
10 reasonable person.

11 122. Defendant lacked a legitimate business interest in causing the placement and/or
12 transmission of third-party cookies along with user data that allowed the Third Parties to track,
13 intercept, receive, and collect Private Communications, including their browsing history, visit
14 history, website interactions, user input data, demographic information, interests and
15 preferences, shopping behaviors, device information, referring URLs, session information, user
16 identifiers, and/or geolocation data, without their consent.

17 123. Plaintiffs and Class members have been damaged by Defendant's invasion of
18 their privacy and are entitled to just compensation, including monetary damages.

19 124. Plaintiffs and Class members seeks appropriate relief for that injury, including
20 but not limited to, damages that will compensate them for the harm to their privacy interests as
21 well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs'
22 and Class members' privacy.

23 125. Plaintiffs and Class members seek punitive damages because Defendant's
24 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and
25 Class members and made in conscious disregard of Plaintiffs' and Class members' rights and
26 Plaintiffs' and Class members' declination or rejection of the Website's use of non-required
27 cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.
28

Second Cause of Action: Intrusion Upon Seclusion

126. Plaintiffs reallege and incorporates by reference all paragraphs alleged herein.

127. To assert a claim for intrusion upon seclusion, Plaintiffs must plead (i) that Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs had a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a reasonable person.

128. By permitting third-party cookies to be stored on consumers' devices without consent, which caused the Third Parties to track and collect Plaintiffs' and Class members' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, in violation of Defendant's representations otherwise in the popup cookie consent banner, Defendant intentionally intruded upon the solitude or seclusion of Website users. Defendant effectively placed the Third Parties in the middle of communications to which they were not invited, welcomed, or authorized.

129. The Third Parties' tracking and collecting of Plaintiffs' and Class member's Private Communications on the Website using third-party cookies that Defendant caused to be stored on users' devices—and to be transmitted to Third Parties—was not authorized by Plaintiffs and Class members, and, in fact, those Website users specifically chose to opt out of, decline, or reject non-required cookies.

130. Plaintiffs and the Class members had an objectively reasonable expectation of privacy surrounding his and their Private Communications on the Website based on Defendant's promise that users could opt out of, decline, or reject non-required cookies, as well as state criminal and civil laws designed to protect individual privacy.

131. Defendant's intentional intrusion into Plaintiffs' and other users' Private Communications would be highly offensive to a reasonable person given that Defendant represented that Website users could "opt out of" or "choose whether this site may use Functional and/or Advertising cookies" when, in fact, Defendant caused such third-party cookies to be

1 stored on consumers' devices and browsers, and to be transmitted to third parties, even when
 2 consumers opted out of, declined, or rejected all such cookies. Indeed, Plaintiffs and Class
 3 members reasonably expected, based on Defendant's false representations, that when they opted
 4 out of, declined, or rejected all non-required cookies and tracking technologies, Defendant would
 5 not cause such third-party cookies to be stored on his and their devices or permit the Third Parties
 6 to obtain their Private Communications on the Website, including their browsing history, visit
 7 history, website interactions, user input data, demographic information, interests and
 8 preferences, shopping behaviors, device information, referring URLs, session information, user
 9 identifiers, and/or geolocation data.

10 132. Defendant's conduct was intentional and intruded on Plaintiffs' and users' Private
 11 Communications on the Website.

12 133. Plaintiffs and Class members have been damaged by Defendant's invasion of
 13 their privacy and are entitled to just compensation, including monetary damages.

14 134. Plaintiffs and Class members seeks appropriate relief for that injury, including
 15 but not limited to, damages that will compensate them for the harm to their privacy interests as
 16 well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs'
 17 and Class members' privacy.

18 135. Plaintiffs and Class members seek punitive damages because Defendant's
 19 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and
 20 Class members and made in conscious disregard of Plaintiffs' and Class members' rights and
 21 Plaintiffs' and Class members' declination or rejection of the Website's use of non-required
 22 cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

23 **Third Cause of Action: Wiretapping in Violation of the California Invasion of**
 24 **Privacy Act (California Penal Code § 631)**

25 136. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

26 137. California Penal Code § 631(a) provides, in pertinent part:

27 “Any person who, by means of any machine, instrument, or contrivance, or
 28 in any other manner . . . willfully and without the consent of all parties to
 the communication, or in any unauthorized manner, reads, or attempts to

read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars”

138. The California Supreme Court has repeatedly stated an “express objective” of CIPA is to “protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call.” *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

139. Further, as the California Supreme Court has held, in explaining the legislative purpose behind CIPA:

While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device*.

As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (emphasis supplied; internal citations omitted).

140. CIPA § 631(a) imposes liability for “distinct and mutually independent patterns of conduct.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under § 631(a), Plaintiffs need only establish that Defendant, “by means of any machine, instrument, contrivance, or in any other manner,” did **any** of the following:

[i] Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;

[ii] Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;

[iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

1 Cal. Penal Code § 631(a).

2 141. CIPA § 631(a) also penalizes those who [iv] “aid[], agree[] with, employ[], or
3 conspire[] with any person” who conducts the aforementioned wiretapping, or those who
4 “permit” the wiretapping.

5 142. Defendant is a “person” within the meaning of California Penal Code § 631.

6 143. Section 631(a) is not limited to phone lines, but also applies to “new
7 technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL
8 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be
9 construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v.*
10 *Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic
11 communications”); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31,
12 2022) (“Though written in terms of wiretapping, Section 631(a) applies to Internet
13 communications.”).

14 144. The Third Parties’ cookies—as well as the software code of the Third Parties
15 responsible for placing the cookies and transmitting data from user devices to the Third Parties—
16 constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA (and, even if they do
17 not, Defendant’s deliberate and purposeful scheme that facilitated the interceptions falls under
18 the broad statutory catch-all category of “any other manner”).

19 145. Each of the Third Parties is a “separate legal entity that offers [a] ‘software-as-a-
20 service’ and not merely a passive device.” *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D.
21 Cal. 2021). Further, the Third Parties had the capability to use the wiretapped information for
22 their own purposes and, as alleged above, they did in fact use the wiretapped information for
23 their own business purposes. Accordingly, the Third Parties were third parties to any
24 communication between Plaintiffs and Class members, on the one hand, and Defendant, on the
25 other. *Id.* at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal.
26 2023).

1 146. Under § 631(a), Defendant must show it had the consent of all parties to a
2 communication.

3 147. At all relevant times, the Website caused Plaintiffs and Class members' browsers
4 to store the Third Parties' cookies and to transmit those cookies alongside Private
5 Communications—including their browsing history, visit history, website interactions, user
6 input data, demographic information, interests and preferences, shopping behaviors, device
7 information, referring URLs, session information, user identifiers, and/or geolocation data—to
8 the Third Parties without Plaintiffs' and Class members' consent. By configuring the Website in
9 this manner, Defendant willfully aided, agreed with, employed, permitted, or otherwise caused
10 the Third Parties to wiretap Plaintiffs and Class members using the Third Parties' cookies and to
11 accomplish the wrongful conduct alleged herein.

12 148. At all relevant times, by their cookies and corresponding software code, the Third
13 Parties willfully and without the consent of all parties to the communication, or in any
14 unauthorized manner, read, attempted to read, and/or learned the contents or meaning of
15 electronic communications of Plaintiffs and Class members, on the one hand, and Defendant, on
16 the other, while the electronic communications were in transit or were being sent from or
17 received at any place within California.

18 149. The Private Communications of Plaintiffs and Class members, on the one hand,
19 and Defendant, on the other, that the Third Parties automatically intercepted directly
20 communicates the Website user's affirmative decisions, actions, choices, preferences, and
21 activities, which constitute the "contents" of electronic communications, including their
22 browsing history, visit history, website interactions, user input data, demographic information,
23 interests and preferences, shopping behaviors, device information, referring URLs, session
24 information, user identifiers, and/or geolocation data.

25 150. At all relevant times, the Third Parties used or attempted to use the Private
26 Communications automatically intercepted by their cookie tracking technologies for their own
27 purposes.
28

1 151. Plaintiffs and Class members did not provide their prior consent to the Third
2 Parties' intentional access, interception, reading, learning, recording, collection, and usage of
3 Plaintiffs' and Class members' electronic communications. Nor did Plaintiffs and Class members
4 provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or
5 otherwise causing the Third Parties' conduct. On the contrary, Plaintiffs and Class members
6 expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept,
7 read, learn, record, collect, and use Plaintiffs' and Class members' electronic communications
8 by choosing to opt out of, decline, or reject non-required cookies in the Your Choices window.

9 152. The wiretapping of Plaintiffs and Class members occurred in California, where
10 Plaintiffs and Class members accessed the Website and where the Third Parties—as caused by
11 Defendant—routed Plaintiffs' and Class members' electronic communications to Third Parties'
12 servers. Among other things, the cookies, as well as the software code responsible for placing
13 the cookies and transmitting them and other Private Communications to the Third Parties, resided
14 on Plaintiffs' California-located device. In particular, the user's California-based device, after
15 downloading the software code from the Third Parties' servers, (i) stored the code onto the user's
16 disk; (ii) converted the code into machine-executable format; and (iii) executed the code, causing
17 the transmission of data (including cookie data) to and from the Third Parties.

18 153. Plaintiffs and Class members have suffered loss by reason of these violations,
19 including, but not limited to, (i) violation their right to privacy, (ii) loss of value in their Private
20 Communications, (iii) damage to and loss of Plaintiffs' and Class members' property right to
21 control the dissemination and use of their Private Communications, and (iv) loss of their Private
22 Communications to the Third Parties with no consent.

23 154. Pursuant to California Penal Code § 637.2, Plaintiffs and Class members have
24 been injured by the violations of California Penal Code § 631, and each seeks statutory damages
25 of the greater of \$5,000, or three times the amount of actual damages, for each of Defendant's
26 violations of CIPA § 631(a), as well as injunctive relief.

1 155. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein
 2 including, but not limited to, permitting third parties to access, intercept, read, learn, record,
 3 collect, and use Plaintiffs' and Class members' electronic Private Communications with
 4 Defendant. Plaintiffs, Class members, and the general public continue to be at risk because
 5 Plaintiffs, Class members, and the general public frequently use the internet to search for
 6 information and content related to fitness and nutrition trackers and related products and services.
 7 Plaintiffs, Class members, and the general public continue to desire to use the internet for that
 8 purpose. Plaintiffs, Class members, and the general public have no practical way to know if their
 9 request to decline or reject non-required cookies and tracking technologies will be honored
 10 and/or whether Defendant will permit third parties to access, intercept, read, learn, record,
 11 collect, and use Plaintiffs' and Class members' electronic Private Communications with
 12 Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read,
 13 learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications
 14 with Defendant and will continue to do so unless and until enjoined.

15 **Fourth Cause of Action: Use of a Pen Register in Violation of the California**
 16 **Invasion of Privacy Act (California Penal Code § 638.51)**

17 156. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

18 157. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to
 19 638, includes the following statement of purpose:

20 The Legislature hereby declares that advances in science and technology have led
 21 to the development of new devices and techniques for the purpose of
 22 eavesdropping upon private communications and that the invasion of privacy
 resulting from the continual and increasing use of such devices and techniques
 has created a serious threat to the free exercise of personal liberties and cannot be
 tolerated in a free and civilized society.

23 158. California Penal Code Section 638.51(a) proscribes any "person" from
 24 "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court
 25 order."

26 159. A "pen register" is a "a device or process that records or decodes dialing, routing,
 27 addressing, or signaling information transmitted by an instrument or facility from which a wire
 28

1 or electronic communication is transmitted, but not the contents of a communication.” Cal. Penal
2 Code § 638.50(b).

3 160. The Third Parties’ cookies and the corresponding software code installed by
4 Defendant on its Website are each “pen registers” because they are “device[s] or process[es]”
5 that “capture[d]” the “routing, addressing, or signaling information”—including, the IP address
6 and user-agent information—from the electronic communications transmitted by Plaintiffs’ and
7 the Class’s computers or devices. Cal. Penal Code § 638.50(b).

8 161. At all relevant times, Defendant caused the Third Parties’ cookies and the
9 corresponding software code—which are pen registers—to be placed on Plaintiffs’ and Class
10 members’ browsers and devices, and/or to be used to transmit Plaintiffs’ and Class members’ IP
11 address and user-agent information. *See Greenley v. Kochava*, 2023 WL 4833466, at *15-16
12 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11 (N.D.
13 Cal. Oct. 21, 2024).

14 162. Some of the information collected by the Third Parties’ cookies and the
15 corresponding software, including IP addresses and user-agent information, does not constitute
16 the content of Plaintiffs’ and the Class members’ electronic communications with the Website.
17 *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). (“IP addresses constitute
18 addressing information and do not necessarily reveal any more about the underlying contents of
19 communication...”)(cleaned up).

20 163. Plaintiffs and Class members did not provide their prior consent to Defendant’s
21 use of third-party cookies and the corresponding software. On the contrary, Plaintiffs and the
22 Class members informed Defendant that they did not consent to the Website’s use of third-party
23 cookies by clicking the “here” link in the cookie consent banner and adjusting all available
24 settings to opt out of, decline, or reject non-required cookies in the Your Choices window.

25 164. Defendant did not obtain a court order to install or use the third-party cookies and
26 corresponding software to track and collect Plaintiffs’ and Class member’s IP addresses and
27 user-agent information.
28

1 165. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class
2 members suffered losses and were damaged in an amount to be determined at trial.

3 166. Pursuant to Penal Code § 637.2(a)(1), Plaintiffs and Class members are also
4 entitled to statutory damages of \$5,000 for each of Defendant's violations of § 638.51(a).

5 **Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation**

6 167. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

7 168. Defendant fraudulently and deceptively informed Plaintiffs and Class members
8 that they could "opt out of" cookies or "choose whether this site may use Functional and/or
9 Advertising cookies[.]"

10 169. However, despite Defendant's representations otherwise, Defendant caused third-
11 party cookies and software code to be stored on consumers' devices, and to be transmitted to the
12 Third Parties alongside Private Communications, even after users clicked the "here" link in the
13 popup cookie consent banner. These cookies and corresponding software code allowed the Third
14 Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members'
15 Private Communications, even when consumers had previously chosen to opt out of, decline, or
16 reject non-required cookies.

17 170. These misrepresentations and omissions were known exclusively to, and actively
18 concealed by Defendant, not reasonably known to Plaintiffs and Class members, and material at
19 the time they were made. Defendant knew, or should have known, how the Website functioned,
20 including the Third Party's resources it installed on the Website and the third-party cookies in
21 use on the Website, through testing the Website, evaluating its performance metrics by means of
22 its accounts with the Third Parties, or otherwise, and knew, or should have known, that the
23 Website's programming allowed the third-party cookies to be placed on users'—including
24 Plaintiffs'—browsers and devices and/or transmitted to the Third Parties along with users'
25 Private Communications even after users attempted to opt out of, decline, or reject non-required
26 cookies, which Defendant promised its users they could do. Defendant's misrepresentations and
27 omissions concerned material facts that were essential to the analysis undertaken by Plaintiffs
28

1 and Class members as to whether to use the Website. In misleading Plaintiffs and Class members
2 and not so informing them, Defendant breached its duty to Plaintiffs and Class members.
3 Defendant also gained financially from, and as a result of, its breach.

4 171. Plaintiffs and Class members relied to their detriment on Defendant's
5 misrepresentations and fraudulent omissions.

6 172. Plaintiffs and Class members have suffered an injury-in-fact, including the loss
7 of money and/or property, as a result of Defendant's unfair, deceptive, and/or unlawful practices,
8 including the unauthorized interception of their Private Communications, including their
9 browsing history, visit history, website interactions, user input data, demographic information,
10 interests and preferences, shopping behaviors, device information, referring URLs, session
11 information, user identifiers, and/or geolocation data, which have value as demonstrated by the
12 use and sale of consumers' browsing activity, as alleged above. Plaintiffs and Class members
13 have also suffered harm in the form of diminution of the value of their private and personally
14 identifiable information and communications.

15 173. Defendant's actions caused damage to and loss of Plaintiffs' and Class members'
16 property right to control the dissemination and use of their personal information and
17 communications.

18 174. Defendant's representation that consumers could opt out of, decline, or reject
19 non-required cookies (including those used "for analytics (Functional Cookies), and to
20 personalize content and ads (Advertising Cookies)") if they adjusted all available settings in the
21 Your Choices window was untrue. Again, had Plaintiffs and Class members known these facts,
22 they would not have used the Website. Moreover, Plaintiffs and Class members reviewed the
23 popup cookie consent banner and Your Choices window prior to their interactions with the
24 Website. Had Defendant disclosed that it caused third-party non-required cookies to be stored
25 on Website visitors' devices that are related to personalization, advertising, and analytics and/or
26 share information with third parties even after they choose to opt out of, decline, or reject all
27
28

1 such non-required cookies, Plaintiffs and Class members would have noticed it and would not
2 have interacted with the Website.

3 175. By and through such fraud, deceit, misrepresentations and/or omissions,
4 Defendant intended to induce Plaintiffs and Class members to alter their positions to their
5 detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiffs and Class
6 members to, without limitation, use the Website under the mistaken belief that Defendant would
7 not permit third parties to obtain users' Private Communications when consumers chose to opt
8 out of, decline, reject non-required cookies. As a result, Plaintiffs and the Class provided more
9 personal data than they would have otherwise.

10 176. Plaintiffs and Class members justifiably and reasonably relied on Defendant's
11 misrepresentations and omissions, and, accordingly, were damaged by Defendant's conduct.

12 177. As a direct and proximate result of Defendant's misrepresentations and/or
13 omissions, Plaintiffs and Class members have suffered damages, as alleged above, and are
14 entitled to just compensation, including monetary damages.

15 178. Plaintiffs and Class members seek punitive damages because Defendant's
16 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and
17 Class members and made in conscious disregard of Plaintiffs' and Class members' rights and
18 Plaintiffs' and Class members' declination or rejection of the Website's use of non-required
19 cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

20 **Sixth Cause of Action: Unjust Enrichment**

21 179. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

22 180. Defendant created and implemented a scheme to increase its own profits through
23 a pervasive pattern of false statements and fraudulent omissions.

24 181. Defendant was unjustly enriched as a result of its wrongful conduct, including
25 through its misrepresentations that users could "opt out of" or "choose whether this site may use
26 Functional and/or Advertising cookies" and by permitting the Third Parties to store and transmit
27 cookies on Plaintiffs' and Class members' devices and browsers, which permitted the Third
28

Parties to track and collect users' Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even after Class members rejected non-required cookies.

182. Plaintiffs and Class members' Private Communications have conferred an economic benefit on Defendant.

183. Defendant has been unjustly enriched at the expense of Plaintiffs and Class members, and Defendant has unjustly retained the benefits of its unlawful and wrongful conduct.

184. Defendant appreciated, recognized, and chose to accept the monetary benefits that Plaintiffs and Class members conferred onto Defendant at his and their detriment. These benefits were the expected result of Defendant acting in its pecuniary interest at the expense of Plaintiffs and Class members.

185. It would be unjust for Defendant to retain the value of Plaintiffs' and Class members' property and any profits earned thereon.

186. There is no justification for Defendant's enrichment. It would be inequitable, unconscionable, and unjust for Defendant to be permitted to retain these benefits because the benefits were procured as a result of its wrongful conduct.

187. Plaintiffs and Class members are entitled to restitution of the benefits Defendant unjustly retained and/or any amounts necessary to return Plaintiffs and Class members to the position they occupied prior to having their Private Communications tracked and collected by the Third Parties.

188. Plaintiffs plead this claim separately, as well as in the alternative, to their other claims, as without such claims Plaintiffs would have no adequate legal remedy.

Seventh Cause of Action: Trespass to Chattels

189. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

190. Defendant, intentionally and without consent or other legal justification, caused cookies to be stored on Plaintiffs' and Class members' browsers and devices, which caused the

1 Third Parties and Defendant to track and collect Plaintiffs' and Class members' Private
2 Communications and use the data collected for their own advantage, as described above.

3 191. Defendant was unjustly enriched as a result of its wrongful conduct, including
4 through its misrepresentation that users could opt out of, decline, or reject all non-required
5 cookies and tracking technologies, and through their failure to disclose that Defendant causes
6 third-party cookies to be stored on consumers' devices and browsers, which cause the Third
7 Parties and Defendant to track and collect Plaintiffs' and Class members' Private
8 Communications even after consumers chose to opt out of, decline, or reject such cookies.

9 192. Defendant intentionally caused third party software code to be stored onto
10 Plaintiffs' and Class members' devices, knowing that the code would be executed by those
11 devices. The software code then placed and/or transmitted cookies along with Plaintiffs' and
12 Class members' Private Communications to the Third Parties. These intentional acts interfered
13 with Plaintiffs' and Class members' use of the following personal property owned, leased, or
14 controlled by Plaintiffs and other users: (a) his and their computers and other electronic devices;
15 and (b) his and their personally identifiable information.

16 193. Defendant's trespass of Plaintiffs' and other users' computing devices resulted in
17 harm to Plaintiffs and other users and caused Plaintiffs and other users the following damages:

- 18 a. Nominal damages for trespass;
19 b. Reduction of storage, disk space, and performance of Plaintiffs' and other users'
20 computing devices; and
21 c. Loss of value of Plaintiffs' and other users' computing devices.

22 **PRAYER FOR RELIEF**

23 **WHEREFORE**, reserving all rights, Plaintiffs, on behalf of themselves and the Class
24 members, respectfully request judgment against Defendant as follows:

- 25 A. Certification of the proposed Class, including appointment of Plaintiffs' counsel
26 as class counsel;
27
28

1 B. An award of compensatory damages, including statutory damages where
2 available, to Plaintiffs and Class members against Defendant for all damages sustained as a result
3 of Defendant's wrongdoing, including both pre- and post-judgment interest thereon;

4 C. An award of punitive damages;

5 D. An award of nominal damages;

6 E. An order for full restitution;

7 F. An order requiring Defendant to disgorge revenues and profits wrongfully
8 obtained;

9 G. An order temporarily and permanently enjoining Defendant from continuing the
10 unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

11 H. For reasonable attorneys' fees and the costs of suit incurred; and

12 I. For such further relief as may be just and proper.

13 Dated: May 22, 2025

14 **GUTRIDE SAFIER LLP**

15 /s/ Seth A. Safier

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

16 Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

17 Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

18 Kali R. Backer (State Bar No. 342492)

kali@gutridesafier.com

19 100 Pine Street, Suite 1250

San Francisco, CA 94111

20 Telephone: (415) 639-9090

21 Facsimile: (415) 449-6469

22 *Attorneys for Plaintiffs*